National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

VIRTUAL PRIVATE NETWORK CAPABILITY PACKAGE

This Commercial Solutions for Classified (CSfC) Capability Package describes how to protect classified data in transit across an untrusted network using a virtual private network (VPN) implemented with multiple layers of Internet Protocol Security (IPsec) encryption.

Version 2.08
December 19, 2013

CHANGE HISTORY

Title	Version	Date	Change Description
Commercial Solutions for Classified (CSfC) Multi-Site Virtual Private Network (VPN) Capability Package	0.8	March 14, 2012	• Initial release of CSfC Virtual Private Network (VPN) guidance.
Commercial Solutions for Classified (CSfC) Multi-Site Virtual Private Network (VPN) Capability Package	1.0	August 17, 2012	• Official release of CSfC VPN guidance. • Adjudicated public review of Multi-Site VPN CP 0.8.
Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package	1.08	March 4, 2013	• Initial release of CSfC VPN guidance for remote access. • Added Remote Access Architecture and associated requirements and test procedures. • Split compound requirements into separate requirements. • Assigned requirement identifiers to “shall” statements in Sections 4 and 5 of Multi-Site VPN CP 1.0. • Explicitly identified which requirements apply to each architecture. • Explicitly identified threshold and objective requirements.
Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package	2.0	May 28, 2013	• Official release of CSfC VPN guidance. • Added requirements for using a single VPN solution for networks of multiple security levels. • Added use cases for End User Devices (EUDs) in non-remote-access scenarios. • Split and renumbered compound requirements.

Title	Version	Date	Change Description
Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package	2.08	December 19, 2013	• Initial release of CSfC VPN guidance for use of a single Gray network with networks of multiple security levels. • Initial release of CSfC VPN guidance for distribution of Certificate Revocation Lists (CRLs) on the external side of VPN Components. • Added additional requirements for the content and distribution of CRLs.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The Capability Packages are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators.

IAD is delivering a generic CSfC Virtual Private Network (VPN) Capability Package to meet the demand for data in transit solutions using a secure sharing suite (S3) of algorithms [NSA Suite B]. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. VPN Capability Package Version 2.08 enables customers to implement VPNs between two or more sites and VPNs between fixed sites and End User Devices (EUDs). This Capability Package takes lessons learned from five proof-of-concept demonstrations that had implemented a set of S3 algorithms, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

This version of the CSfC VPN Capability Package does **not** supersede the CSfC VPN Capability Package Version 2.0 dated May 28, 2013. A future version of this Capability Package, expected to be released as Version 3.0, is intended to supersede the CSfC VPN Capability Package Version 2.0. Until the release of Version 3.0, the CSfC VPN Capability Package Version 2.0 dated May 28, 2013 remains approved by the IAD Director and is the preferred Capability Package to be used for implementing a CSfC VPN solution.

2 PURPOSE OF THIS DOCUMENT

This Capability Package provides reference architectures and corresponding configuration information that allows customers to select COTS products from the CSfC Components List for their VPN solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 10, customers must ensure that the components selected from the CSfC Components List will permit the necessary functionality for the selected architecture. Throughout this document, requirements imposed on the VPN solution are identified by a label consisting of the prefix “VPN,” a two-letter category, and a sequence number (e.g., VPN-KM-11). To successfully implement a solution based on this Capability Package, all Threshold requirements, or the corresponding Objective requirements, applicable to the selected architectures must be implemented, as described in Section 8.

Customers who want to use the solution detailed in this Capability Package must contact NSA to determine ways to obtain NSA approval. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

3 USE OF THIS DOCUMENT

This document may not be used for a CSfC solution without formally obtaining support from NSA for the effort prior to presenting a solution to the implementing organization's Authorizing Official (AO). United States Government entities interested in presenting solutions to their AOs in accordance with this guidance must first obtain NSA support by submitting a request for Capability Package application support to their NSA/IAD Client Advocate. In the future, however, customers and their solution providers will be able to use a later version of this guidance to implement solutions without such NSA/IAD involvement. Until that time, customers and solution providers may still register solutions designed according to Version 2.0 of the VPN Capability Package, dated May 28, 2013; see Section 3 of that document for details.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the VPN Capability Package maintenance team at vpn@nsa.gov.

The following Legal Disclaimer relates to the use of this Capability Package:

This Capability Package is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Capability Package, even if advised of the possibility of such damage.

The User of this Capability Package agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this Capability Package is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 DESCRIPTION OF THE VPN SOLUTION

This Capability Package describes a general VPN solution to protect classified information as it travels across either an untrusted network or a network of a different classification level. The solution supports interconnecting two or more networks operating at the same security level via a VPN, where the security level encompasses the classification level, list of compartments, dissemination controls, and other such controls over information. The solution also supports connecting individual devices, referred

to in this Capability Package as End User Devices (EUDs), to a network via the VPN solution, provided that the device and the network operate at the same security level. The solution provides sufficient flexibility to be applicable to many use cases of VPN implementations.

The VPN solution uses two nested, independent Internet Protocol Security (IPsec) tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two IPsec tunnels protecting a data flow are generated by VPN Gateways implemented as part of the network infrastructure or by VPN Client software running on an EUD. Throughout this Capability Package, the term "VPN Component" is used to refer generically to VPN Gateways and VPN Clients alike, in situations where the differences between the two are unimportant.

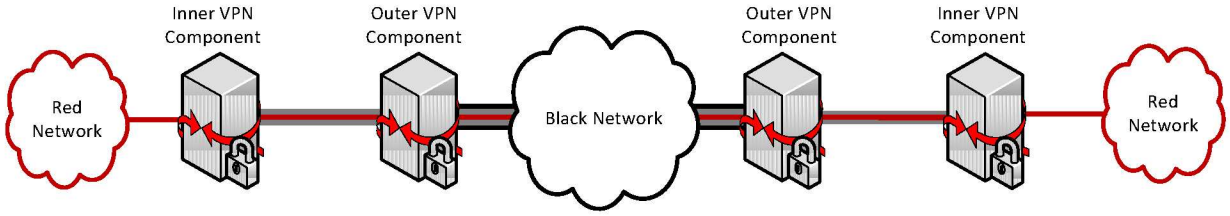


Figure 1. Two IPsec Tunnels Protect Data across an Untrusted Network

As shown in Figure 1, before being sent across the untrusted network, each packet of classified data is encrypted twice: first by an Inner VPN Component, and then by an Outer VPN Component. At the other end of the data flow, the received packet is correspondingly decrypted twice: first by an Outer VPN Component, and then by an Inner VPN Component.

4.1 NETWORKS

The following terms are used throughout this document to refer to the various types of networks that appear in a VPN solution.

4.1.1 RED NETWORK

A Red network contains unencrypted classified data and is logically located behind an Inner VPN Gateway. The networks connected to one another through the VPN solution are each Red networks. Red networks are under the control of the solution owner or a trusted third party. Red networks may only communicate with one another through the VPN solution if the networks operate at the same security level.

4.1.2 GRAY NETWORK

A Gray network contains classified data that has been encrypted once. The network between an Inner VPN Gateway and an Outer VPN Gateway is a Gray network. Gray networks are under the control of the solution owner or a trusted third party. Gray networks are either physically or cryptographically divided into two sub-networks, as follows:

- Gray Management network – The part of a Gray network that contains the management functions to run components supporting the Outer layer of IPsec, including the Outer tunnel Certificate Authority (CA) and the Outer VPN Gateway admin and audit server functions.
- Gray Data network – The part of a Gray network that carries data between Inner and Outer VPN Components.

4.1.3 BLACK NETWORK

A Black network contains classified data that has been encrypted twice. The network connecting the Outer VPN Components together is a Black network. Black networks are not necessarily (and often will not be) under the control of the solution owner, and may be operated by an untrusted third party.

4.2 INTEROPERABILITY

The VPN solution defined in this Capability Package supports interoperability by having similar standards-based configurations at both ends of each layer of the solution. However, there is no guarantee of generic interoperability between any two products on the CSfC Components List. An IAD goal is to create and realize adoption of IPsec implementation standards that will allow for this generic interoperability in the future.

4.3 ARCHITECTURE

The VPN solution is adaptable to multiple architectures, depending on the needs of the customer implementing the solution. If a customer does not have a need for EUDs or for multiple security levels, then they need not be included as part of the implementation. Similarly, a customer may implement a pure remote access solution consisting of a single site plus some number of EUDs, in which case there will be no communications between multiple sites. However, any implementation of the VPN solution must satisfy all of the applicable requirements specified in this Capability Package.

4.3.1 MULTIPLE SITES

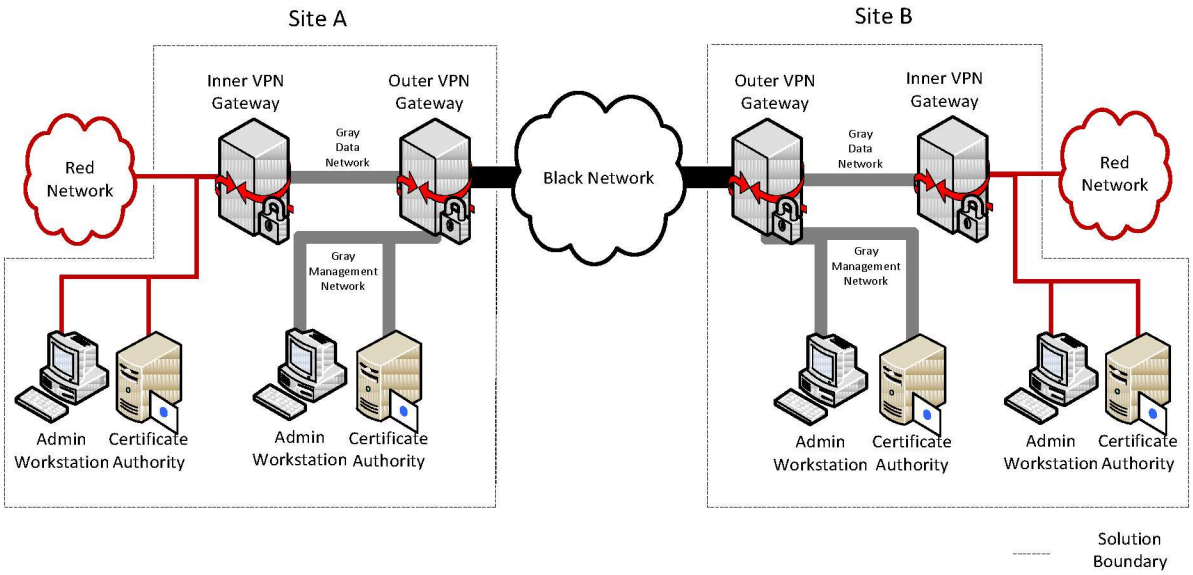


Figure 2. VPN Solution Connecting Two Independently Managed Sites

Figure 2 depicts two Red networks at different sites that operate at the same security level, connected to one another through the VPN solution. Here, each Red network has two VPN Gateways associated with it: an Inner VPN Gateway connected to the Red network, and an Outer VPN Gateway between the Inner VPN Gateway and the Black network. There are two IPsec tunnels between any pair of sites communicating directly with one another: one IPsec tunnel between their Outer VPN Gateways, and a second IPsec tunnel between their Inner VPN Gateways.

There is no limit to the number of sites that may be incorporated into a single VPN solution.

Sites in the solution may be managed independently of one another, or may be remotely managed from a central site.

4.3.1.1 Independently Managed Sites

For independently managed sites, each site performs the administration of its own VPN Gateways and has the option of using either CAs that they control (see Figure 2) or, if available, enterprise CAs. Each site needs to ensure that the VPN Gateways selected interoperate with those at the other sites. In addition, the two VPN Gateways at each site need to have the signing certificates and revocation information for the corresponding CAs used by the other sites in the VPN solution. Since there is no remote management, no management traffic will cross the Black network, encrypted or otherwise.

This architecture requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. This model has the advantage of allowing

communication between larger organizations that have a need to share information while maintaining independence.

Note that while Figure 2 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in the figure.

4.3.1.2 Centrally Managed Sites

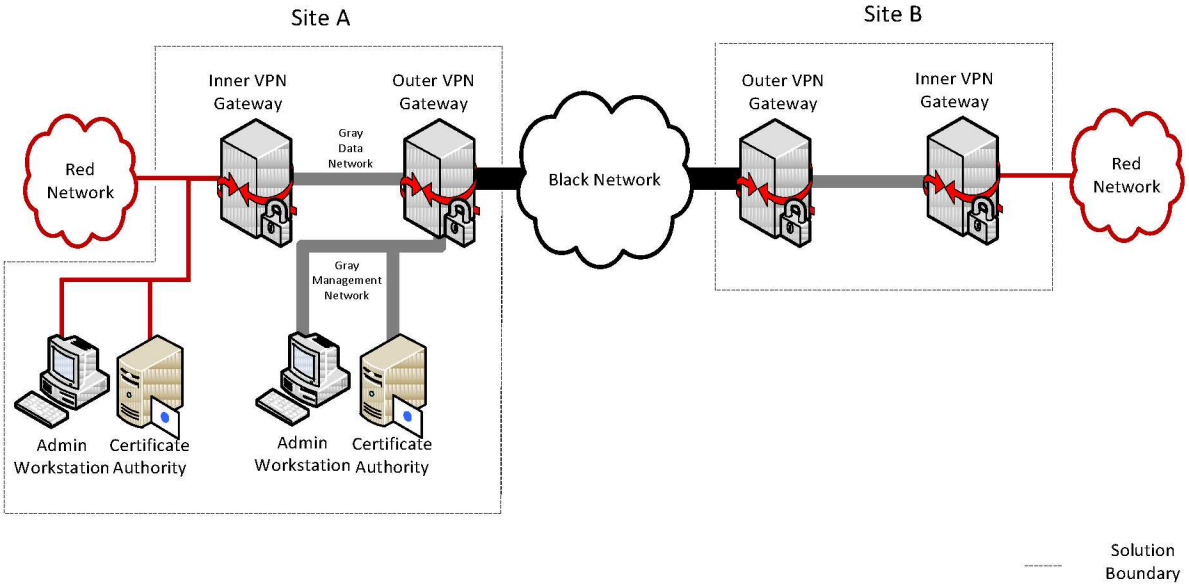


Figure 3. VPN Solution Connecting a Central Management Site and a Remote Site

If remote management is used, personnel at a single geographic site administer and perform keying for all the various sites included in the solution, as shown in Figure 3. In this case, because the administration is done by one group of Security Administrators and CA Administrators (see Section 12), they can ensure the interoperability of each site as new sites are added. Only two CAs are needed: one on the Red network for all the Inner VPN Gateways and one on the Gray Management network for all the Outer VPN Gateways. If available, enterprise CAs may be used.

Because the central management site manages the VPN Gateways at the other sites over the network, encryption is used to logically separate data and management traffic as it passes between sites. Gray management traffic is encrypted using Secure Shell version 2 (SSHv2), Transport Layer Security (TLS), or IPsec before being routed through the Outer VPN Gateway to another site. The SSHv2, TLS, or IPsec serves as the inner layer of encryption for Gray management traffic, and the IPsec tunnel handled by the Outer VPN Gateway serves as the outer layer of encryption. Red management traffic is similarly encrypted before being routed through the Inner and Outer VPN Gateways to another site. As a result, all management traffic between sites is encrypted at least twice before transiting the Black network.

This model makes it easier to add sites because of the centralized administration.

Note that while Figure 3 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same architecture as the remotely managed site in the figure.

4.3.2 End User Devices

An End User Device (EUD) is a device such as a workstation, laptop, or tablet that communicates through the VPN solution to a Red network but is directly connected to a Gray or Black network, rather than being connected to the Red network. There are three possible environments in which EUDs can be used within a VPN solution, with different requirements levied on the EUDs accordingly:

1) An EUD may be located within a secure physical environment and directly connected to a Gray network. Such an EUD must implement an Inner VPN Client to provide the inner layer of IPsec.

2) An EUD may be located within a secure physical environment and directly connected to a Black network. Such an EUD must implement both an Inner VPN Client and an Outer VPN Client to provide both layers of IPsec. (Appendix E describes how an EUD may be designed to implement two VPN Clients together.)

3) An EUD may be located outside of a secure physical environment and directly connected to a Black network. In addition to implementing both an Inner VPN Client and an Outer VPN Client, it must be designed so that it becomes an unclassified device when powered off, and its user must obey additional rules of use to protect the EUD while in operation.

The first two scenarios above enable a customer to use a single physical network infrastructure to carry (singly or doubly) encrypted traffic of multiple security levels, with the EUD encrypting and decrypting packets as they are sent and received. (See Section 5.5.1 for more information about Local EUDs.) The third scenario enables a customer to implement a secure remote access system to allow authorized travelers, teleworkers, and other personnel without ready physical access to a secure facility to access a classified network. (See Section 5.5.2 for more information about Remote EUDs.) This Capability Package addresses all three scenarios, since they have a large number of security requirements in common and share a common infrastructure.

There is no limit to the number of EUDs that may be included in a VPN solution.

When EUDs are incorporated into a VPN solution, the VPN Gateways that the EUDs' VPN Clients will connect to may need to implement VPN headend functionality, which enables the VPN Gateways to assign IP addresses, manage client sessions, and perform other management functions for the VPN Clients. Whether or not the VPN Gateways need to implement headend functionality depends on the choice of VPN Clients used.

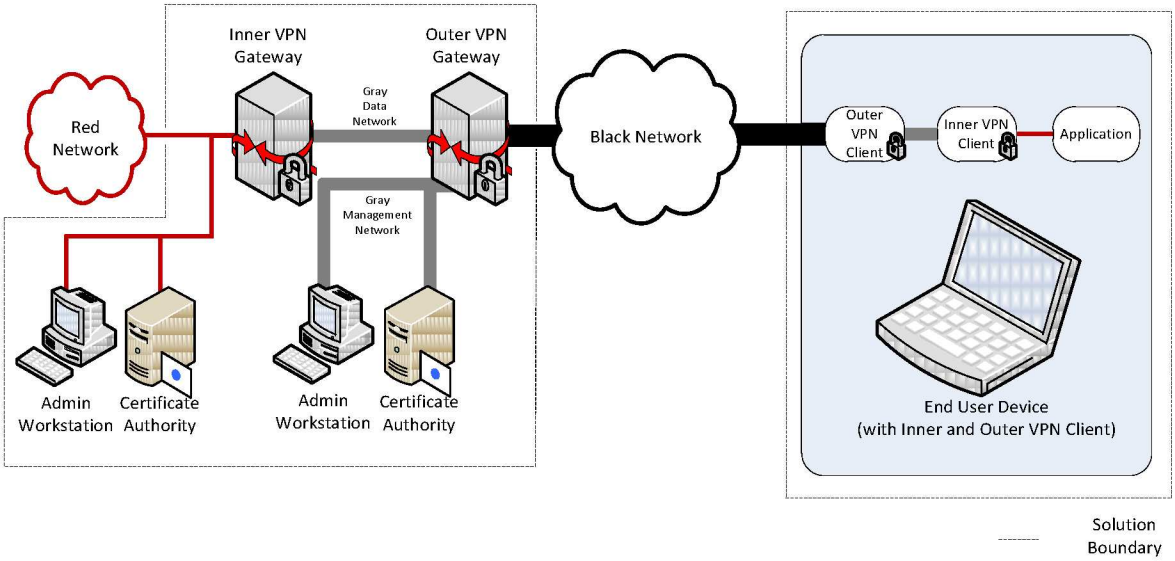


Figure 4. VPN Solution with an EUD Connected to the Black Network

Figure 4 depicts communications between an EUD connected to the Black network and a Red network. The EUD contains two VPN Clients, in order to establish the two nested IPsec tunnels needed to securely communicate with the Red network. The Outer VPN Client on the EUD establishes an IPsec tunnel with the Outer VPN Gateway, and the Inner VPN Client on the EUD establishes an IPsec tunnel with the Inner VPN Gateway.

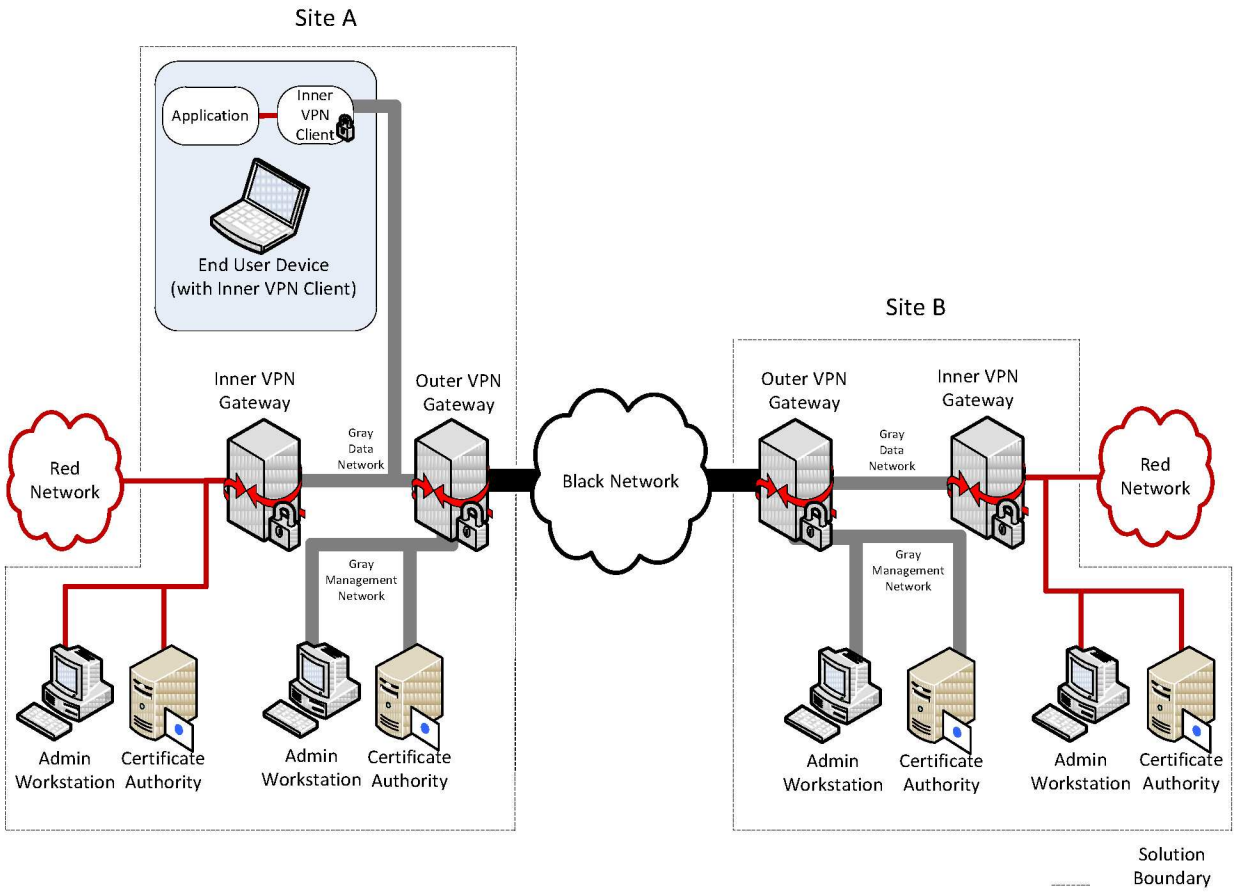


Figure 5. VPN Solution with an EUD Connected to the Gray Network

Figure 5 depicts communications between an EUD connected to the Gray network and Red networks at two different sites. The EUD contains an Inner VPN Client, but not an Outer VPN Client. To communicate with the Red network at Site A, the Inner VPN Client establishes an IPsec tunnel with Site A's Inner VPN Gateway. Traffic between the EUD and Site A's Red network is only encrypted once, but this is acceptable because the data flow is entirely contained within the Gray network and never leaves the control of the system owner. To communicate with the Red network at Site B, the Inner VPN Client establishes an IPsec tunnel with Site B's Inner VPN Gateway. Although the EUD does not implement an Outer VPN Client, the traffic transiting the Black network is still doubly encrypted due to the Outer VPN Gateways connecting Site A's Gray network to Site B's Gray network.

4.3.3 Multiple Security Levels

A single implementation of the VPN solution may support Red networks and EUDs of different security levels, while preventing Red networks and EUDs of differing security levels from communicating with one another. This enables a customer to use the same physical infrastructure to carry traffic from multiple networks. Although each Red network will still require its own Inner VPN Gateway, a site may

use a single Outer VPN Gateway to encrypt and transport traffic that had been encrypted by Inner VPN Components of varying security levels.

There is no limit to the number of different security levels that a VPN solution may support.

Additional security controls are required to maintain separation of singly-encrypted traffic from Red networks of different classification levels. This Capability Package offers two acceptable mechanisms, either of which may be implemented within a solution: physical separation (see Section 4.3.3.2) and stateful traffic filtering firewalls (see Section 4.3.3.3). No additional security controls are needed to separate singly-encrypted traffic from Red networks of the same classification level but different security levels (see Section 4.3.3.1).

VPN solutions supporting multiple security levels may include independently managed sites (see Section 4.3.1.1) or centrally managed sites (see Section 4.3.1.2). In either case, separate CAs and management devices are needed to manage the Inner VPN Components at each security level. For example, Figure 6 depicts a Central Management Site and a Remote Site, but Network A and Network B each have their own CA and management devices, since Networks A and B cannot communicate with one another.

4.3.3.1 Same Classification Level

No additional security controls are needed on the Gray network to maintain separation between singly-encrypted traffic from two or more Red networks that operate at the same classification level.

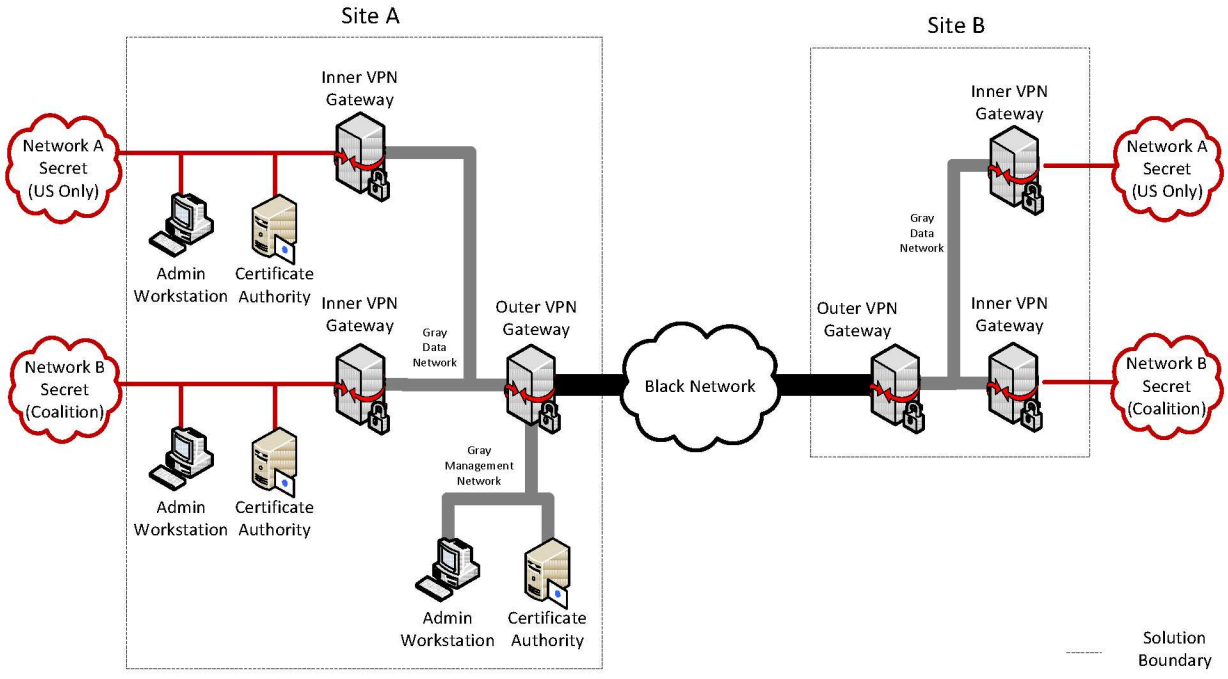


Figure 6. VPN Solution for Two Networks of the Same Classification Level

Figure 6 illustrates a VPN solution between two sites that carries traffic between two Red networks: a Secret U.S.-only network (Network A) and a Secret coalition network (Network B). Because Network A and Network B both operate at the Secret classification level, their singly-encrypted traffic can be carried on the Gray network without any additional security controls in place.

Although not required by this Capability Package, a solution owner may choose to implement the additional security described in Sections 4.3.3.2 or 4.3.3.3 to provide additional mechanisms to prevent unintended data flows between Red networks at the same classification level.

4.3.3.2 Different Classification Levels Separated Physically

One mechanism to enforce separation between singly-encrypted data from two or more Red networks of different classification levels is to use physically separate Gray networks to carry traffic from each classification level. Each Gray network connects to the Outer VPN Gateway using a separate physical port. The Gray CA, Administration Workstation, and other management devices for the Gray network reside either in their own physically separate Gray Management network, or on the Gray network that carries singly-encrypted data of the highest classification level.

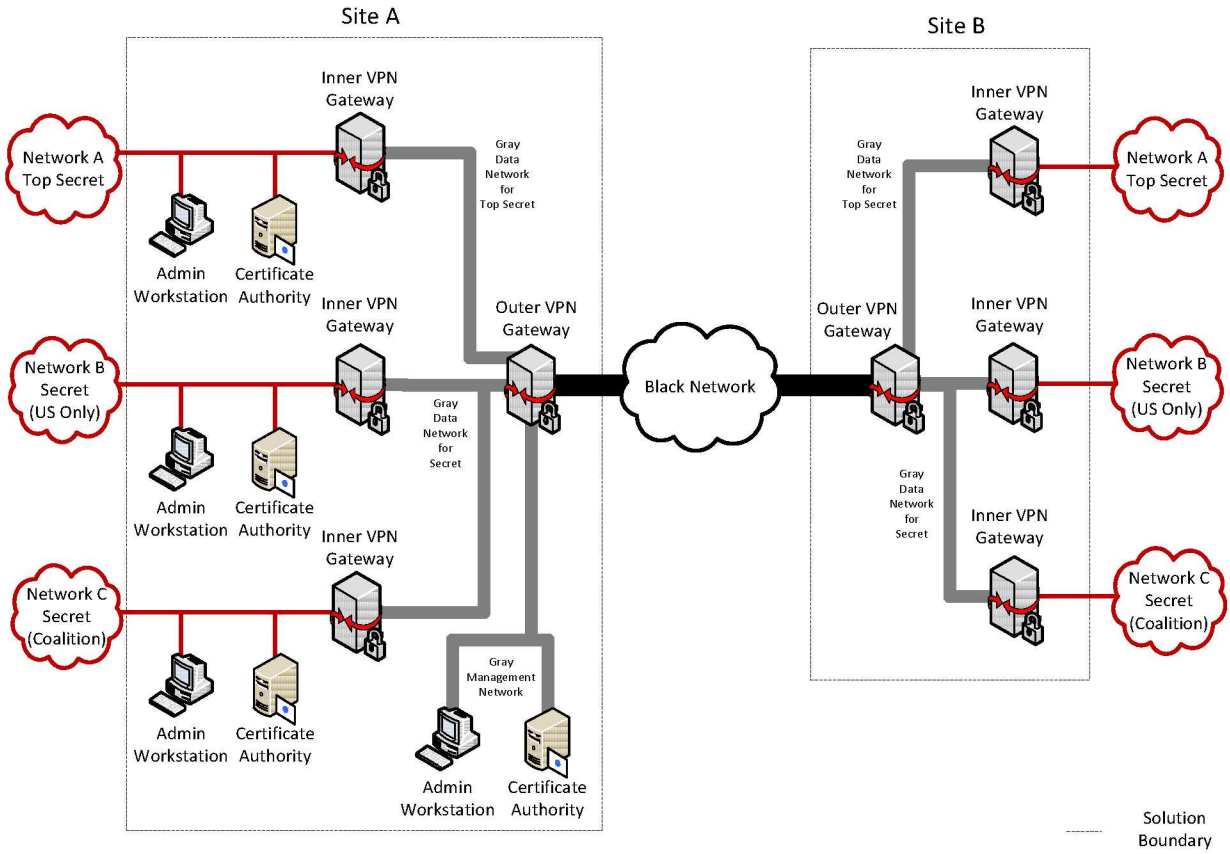


Figure 7. VPN Solution using Physical Separation Between Classification Levels

Figure 7 illustrates a VPN solution between two sites that carries traffic for three different Red networks: a Top Secret network (Network A), a Secret U.S.-only network (Network B), and a Secret coalition network (Network C). Each site implements two Gray networks: one for the two Inner tunnels carrying encrypted traffic from the Top Secret network, and one for the Inner tunnel carrying encrypted traffic from the Secret networks. (Site A also implements a physically separate Gray Management network.) At each site, the two Gray networks connect to the same Outer VPN Gateway, but using separate physical ports. Additional separation between the singly-encrypted data from Network B and Network C is not necessary because they both operate at the same classification level, as described in Section 4.3.3.1.

4.3.3.3 Different Classification Levels Separated via Firewalls

The other acceptable mechanism to enforce separation between singly-encrypted data from two or more Red networks of different classification levels is to add one or more Gray Network Firewalls to the Gray network. These firewalls are placed such that any physical network path between two Inner VPN Components (including those within EUDs) for Red networks of different classification levels must pass through at least one firewall. The Gray Network Firewalls are configured to only allow Inner VPN Components to send packets to one another if they are for Red networks of the same classification level, so that the Gray Network Firewall blocks any traffic flows between two Inner VPN Components of different classification levels.

In order to protect components needed for management of the Gray network, such as the Gray CA and the Gray Administrator Workstation, a Gray Network Firewall must exist along any physical network path between a management component and an Inner VPN Component for a Red network whose classification level is less than the highest classification level protected by the solution, unless the Gray Management network is physically separate from the Gray Data network. A Gray Network Firewall that protects management components may also be used to protect against data flows between classification levels.

This Capability Package provides flexibility in the quantity of Gray Network Firewalls used within the solution and their specific placement within the Gray network, as long as their placement satisfies the above criteria.

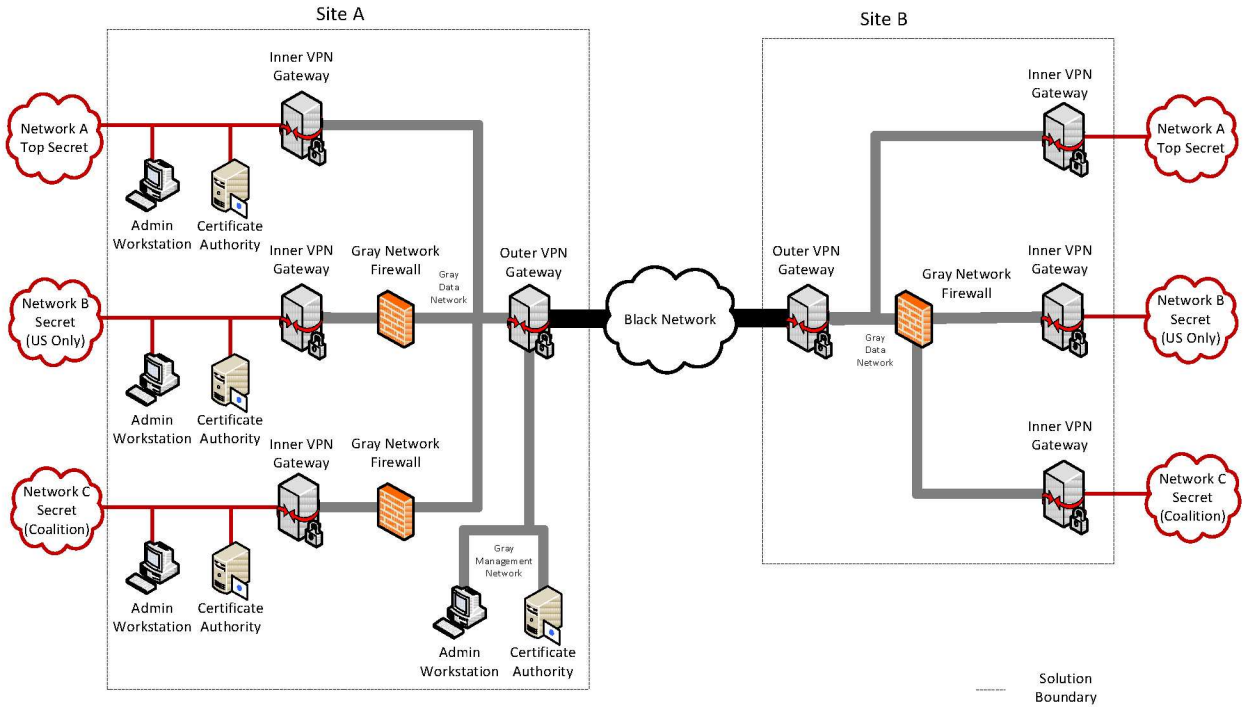


Figure 8. VPN Solution using Firewalls to Enforce Separation Between Classification Levels

Figure 8 illustrates an alternative to the scenario depicted in Figure 7 that uses Gray Network Firewalls instead of physical separation between the Secret and Top Secret networks. Gray Network Firewalls have been placed so that any potential traffic flows between an Inner VPN Gateways for Network A and an Inner VPN Gateway for Network B or C must pass through, and be blocked by, a firewall. Additionally, any potential traffic flows between an Inner VPN Gateway for Network B or C and a device on the Gray Management network must also pass through, and be blocked by, a Gray Network Firewall, even though in this particular example the Gray Management network is physically separate from the Gray Data network. The two sites demonstrate different choices in firewall quantity and placement: Site A uses separate firewalls for Network B and Network C, but Site B uses a single firewall for both.

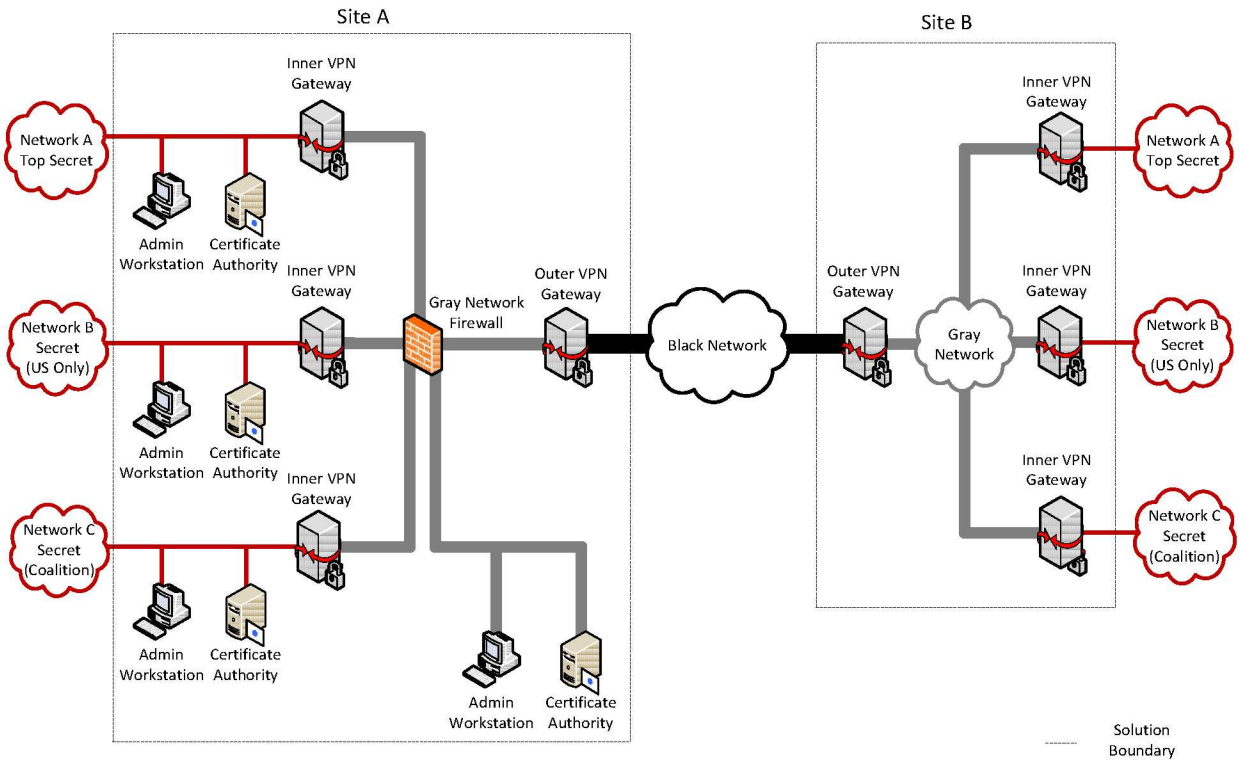


Figure 9. VPN Solution Firewall Placement when Other Site's Details are Unknown

Note that the choice of Gray Network Firewall placement may be complicated if the VPN solution will interconnect with other VPN solutions owned and controlled by other organizations. Details about how one site is maintaining separation of singly-encrypted data from Red networks of different classification levels may not be available to the other site. Because the requirements for Gray Network Firewall placement apply to all physical network paths whether or not they cross solution boundaries, a site that interconnects with another site under independent management and control may choose to position its Gray Network Firewalls such that all traffic on the Gray network to or from the Outer VPN Gateway must pass through them, as illustrated in Figure 9. With this placement, any flows to or from the independently managed site are guaranteed to pass through at least one Gray Network Firewall, regardless of the details of the other site's Gray network architecture. This placement helps insulate Site A from any changes in the layout of Site B's Gray network.

Figure 9 also shows the use of the Gray Network Firewall at Site A to block potential data flows between an Inner VPN Gateway for Network B and C and the CA or Administration Workstation on the Gray network. Unlike the scenario in Figure 8, here the Gray Network Firewall is needed to block those potential flows since there is no physical separation between the Gray Data and Gray Management networks.

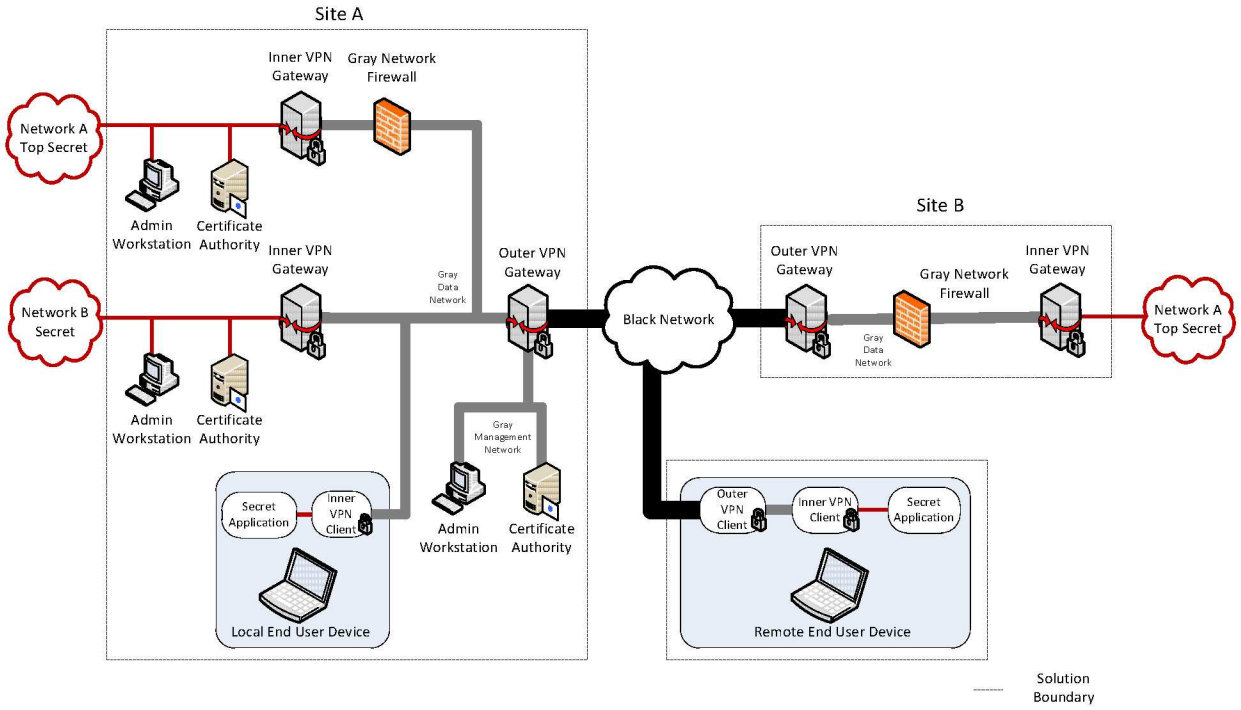


Figure 10. VPN Solution Using Firewalls and EUDs

As an additional example of Gray Network Firewall placement, Figure 10 illustrates a VPN solution that both interconnects Site A and Site B with a Top Secret network and provides Local and Remote EUDs with access to a Secret network. Site A and Site B each include a Gray Network Firewall to ensure that the EUDs, which only operate at the Secret level, are not able to communicate with the Inner VPN Gateways for the Top Secret network. The Gray Management network is physically separated from the Gray Data network, so a Gray Network Firewall between the EUDs and the management components is unnecessary.

4.3.4 External Distribution of Certificate Revocation Lists

Part of the security of the VPN solution depends on the certificate-based mutual authentication that occurs between two VPN Components establishing a VPN tunnel. One step of this mutual authentication entails checking whether the certificate used by the other VPN Component has been revoked, which requires each VPN Component to have access to a current Certificate Revocation List (CRL). As the number of sites interconnected through the VPN solution increases, out-of-band CRL distribution becomes increasingly burdensome and error-prone. Although VPN Components may retrieve the latest CRL directly from the appropriate CA, for Remote Sites this requires first establishing a VPN connection to the Central Management Site where the CAs are located. These additional VPN connections increase the time needed to establish a VPN connection between two Remote Sites. Furthermore, the Remote Site's VPN Components still require out-of-band CRL distribution in order to be able to check for revocation of the certificates used by VPN Components at the Central Management Site, since the VPN

connection to the Central Management Site must be established before the CRLs can be obtained from the CAs.

To avoid these issues, this Capability Package permits the distribution of CRLs on the external side of the VPN Components, which allows the VPN Components to retrieve the current CRL without first establishing a VPN connection. A CDP resides on a different network than the CA that produced the CRL it hosts. An Outer CDP resides on the Black network, and hosts a CRL created by the CA on the Gray network. Similarly, an Inner CDP resides on the Gray network, and hosts a CRL created by the CA on a Red network. Because the CDP and its CA reside on different networks, a one-way transfer mechanism is needed to periodically distribute the current CRL from the CA to the CDP; the details of the one-way transfer mechanism are left to the AO of the solution.

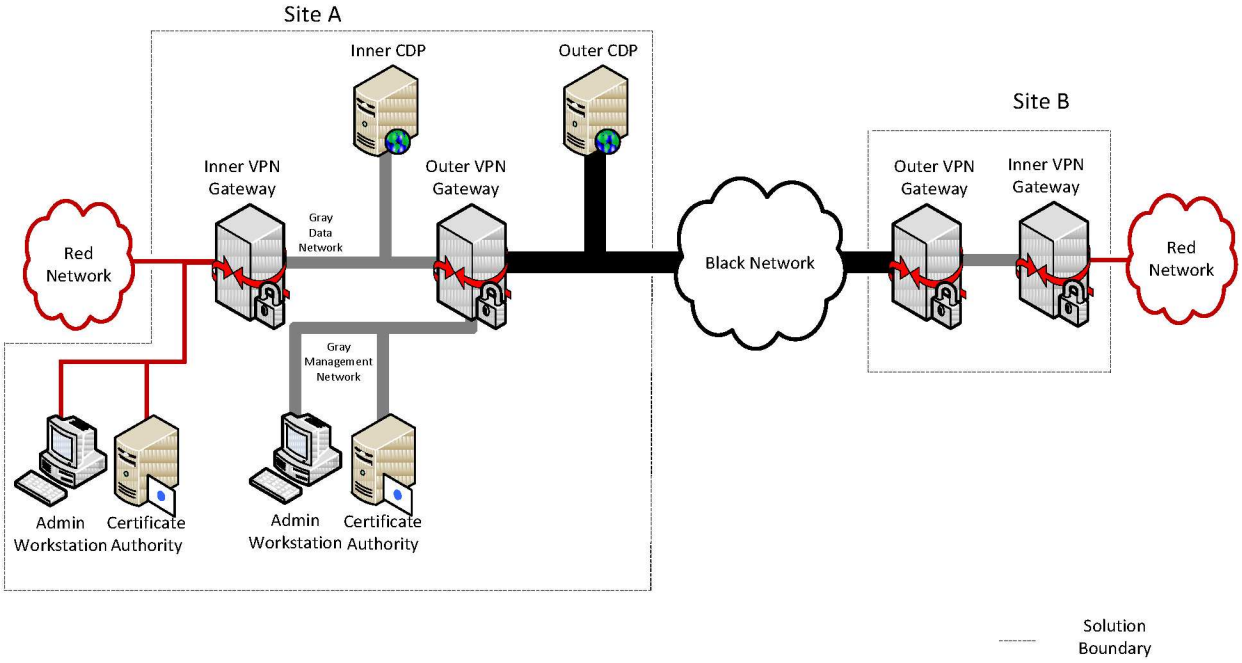


Figure 11. VPN Solution using CRL Distribution Points

Figure 11 illustrates the placement of CDPs to make CRLs accessible to Remote Sites and EUDs on the Black network before VPN tunnel establishment. During negotiation of the outer VPN tunnel, the Outer VPN Components contact the Outer CDP on the Black network to download the latest CRL produced by the Gray CA. Similarly, during negotiation of the inner VPN tunnel, the Inner VPN Components contact the Inner CDP on the Gray network to download the latest CRL produced by the Red CA.

For solutions that support EUDs (see Section 4.3.2), the VPN Clients on an EUD can also download the latest CRLs from the CDPs to check whether the certificates of the VPN Gateways the EUD is connecting to have been revoked. CDPs provide an effective way to quickly distribute CRL updates to Remote EUDs,

since out-of-band CRL distribution to Remote EUDs is expected to be difficult to do in a timely manner, especially for large-scale deployments.

For solutions that support networks of different security levels (see Section 4.3.3), a single Inner CDP may be used to host the CRLs for the Inner VPN Components of multiple Red networks.

A solution owner may choose to implement zero, one, or many CDPs on the Black and Gray networks, based on their expected utility in facilitating CRL distribution to Remote Sites. Having multiple redundant CDPs on the same network improves the availability of CRL distribution, since a VPN Component only needs to be able to contact one CDP in order to obtain the CRL. Conversely, in a small-scale solution, manual out-of-band distribution of CRLs may be more cost-effective than deploying and maintaining CDPs.

4.4 Rationale for Layered Encryption

A single layer of Suite B encryption, properly implemented, is sufficient to protect classified data in transit across an untrusted network. The VPN solution uses two layers of Suite B encryption not because of a deficiency in the cryptographic algorithms themselves, but rather to mitigate the risk that a failure in one of the VPN Components, whether by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability, results in exposure of classified information. The use of multiple layers, implemented with components from different vendors, reduces the likelihood that any one vulnerability can be exploited to attack the full solution, particularly if the layers exhibit suitable independence.

If an Outer VPN Gateway is compromised or fails in some way, the Inner VPN Gateway can still provide the needed encryption for the classified data. In addition, the Inner VPN Gateway can indicate that a failure of the Outer VPN Gateway has occurred, since the filtering rules applied to its Gray network interface will drop and log the receipt of any non-IPsec packets. Such log messages indicate that the Outer VPN Gateway has been breached or misconfigured to permit traffic to pass through to the Inner VPN Gateway that is not allowed.

If instead the Inner VPN Gateway is compromised or fails in some way, the Outer VPN Gateway can likewise still provide the needed encryption for the classified data. As in the previous case, the filtering rules applied to its Gray network interfaces will drop and log the receipt of any non-IPsec packets from the Inner VPN Gateway. Such log messages indicate that the Inner VPN Gateway has been breached or misconfigured to permit traffic to pass through to the Outer VPN Gateway that is not allowed.

If both the Outer and Inner VPN Gateways are compromised or fail simultaneously, then it may be possible for classified data from the Red network to be sent into the Black network without an adequate level of encryption. The security of the VPN solution depends on preventing this failure mode by

remediating any compromises or failures in one VPN Gateway before the other VPN Gateway also fails or is compromised.

4.5 AUTHENTICATION

The VPN solution provides mutual device authentication between VPN Components during tunnel setup via public key certificates, but does not provide any end user authentication for traffic going through the tunnels. In general, any end user authentication between two sites required by the customer must be provided separately and will not be considered as a part of this solution.

As an exception to the above, end user authentication is required when Remote EUDs are being used to provide remote access from outside of a secure physical environment. In this case, the user of the Remote EUD must authenticate to the network before gaining access to any classified data (see requirement VPN-EU-11). The choice of which particular user authentication mechanism to use is left to the customer. End user authentication is not a requirement of this Capability Package for Local EUDs, which are used exclusively within secured facilities approved by the customer.

4.6 PROTOCOLS

Throughout this document, when IP traffic is discussed, it can either be IPv4 or IPv6, unless otherwise specified. In addition, the Red, Gray and Black networks can run either version, and each network is independent from the others in making that decision. In the remainder of the document, if no protocols or standards are specified, then any appropriate protocols may be used to achieve the objective.

Public standards conformant Layer 2 control protocols such as Address Resolution Protocol (ARP) are allowed as necessary to ensure the operational usability of the network. This Capability Package is agnostic with respect to Layer 2; specifically it does not require Ethernet. Public standards conformant Layer 3 control protocols such as Internet Control Message Protocol (ICMP) may be allowed based on local Authorizing Official (AO)/Designated Approving Authority (DAA) policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray network multicast messages and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) may also be allowed depending on local AO/DAA policy. Multicast messages received on external interfaces of the Outer VPN component shall be dropped.

It is expected that the VPN solution can be implemented in such a way as to take advantage of standards based routing protocols that are already being used in the network. For example, networks that currently use Generic Routing Encapsulation (GRE) or Open Shortest Path First (OSPF) protocols can continue to use these in conjunction with this solution to provide routing, provided that the AO/DAA approves their use.

4.7 NETWORK INFRASTRUCTURE

Fundamental network architecture components, such as Domain Name System (DNS) and Network Time Protocol (NTP), are not shown in the figures or explicitly discussed in this document. These components should be located on the inside network of a site (the Gray network for Outer VPN Components and the Red network for the Inner VPN Components). An exception occurs when EUDs are connected to a Black network, in which case basic services on the Black network such as Dynamic Host Configuration Protocol (DHCP) and DNS may initially be necessary for an EUD to join the network and establish a connection to an Outer VPN Gateway.

5 SOLUTION COMPONENTS

In the architectures discussed in the previous section, all communications flowing across the Black network are protected by at least two layers of encryption, implemented using IPsec VPN tunnels generated by VPN Gateways within the network infrastructure and by VPN Clients running on EUDs. Additionally, mandatory aspects of the solution include Administration Workstations and CAs for key management using Public Key Infrastructure (PKI).

Each component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed mandatory for the solution. Overall System Security is discussed in Section 7.

Additional components are discussed in Section 5.8 that can be added to the solution to help reduce the overall risk. However, these are not considered mandatory components for the security of the solution; therefore, this Capability Package does not place configuration or security requirements on the components.

5.1 OUTER VPN GATEWAYS

Authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules are all aspects fundamental to the security provided by VPN Gateways.

The Outer VPN Gateway is located at the edge of the private network and generates an IPsec tunnel, which provides device authentication and confidentiality and integrity of information traversing the Black network. VPNs offer a decreased risk of exposure of information in transit since any information that traverses the Black network is placed in a secure tunnel that provides an authenticated and encrypted path between two sites.

Although the Outer VPN Gateway is a perimeter VPN Gateway and thus more exposed to external attacks, the VPN Gateway is also capable of protecting the network from unauthenticated traffic through use of an internal filtering capability. This allows specification of rules that prohibit

unauthorized data flows, which helps mitigate Denial of Service (DoS) attacks and resource exhaustion. This solution does not require that the Outer VPN Gateway terminate all VPNs on a single physical interface; however, all such external interfaces shall conform to the port filtering requirements in Section 10.6. The Outer VPN Gateway is implemented identically for all the architectures covered in this Capability Package.

In addition to performing the functions described in this Capability Package, an Outer VPN Gateway may also use AO/DAA-approved routing protocols on the Gray network it is connected to. The Outer VPN Gateway cannot route packets between the Gray and Black networks; any packets received on a Gray network interface and sent out a Black network interface must be transmitted within an IPsec VPN tunnel configured according to this Capability Package. There is some data that will originate from the Outer VPN Gateway (such as control traffic (e.g., Bidirectional Forwarding Detection (BFD)), logging and audit data, which will potentially be sent to the Gray Management network at another site) that will only go through the outer IPsec tunnel. This is the only exception to having two layers of encryption for data going over the Black network and is considered acceptable given the limited intelligence value of that information and the fact that it does not contain classified data. However, management traffic on the Gray network, which originates from the Administration Workstation, must include two layers of encryption as described in this Capability Package (see Section 10.8).

5.2 INNER VPN GATEWAYS

Similar to the Outer VPN Gateway, the Inner VPN Gateway provides authentication of peer VPN Components, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules. Unlike the Outer VPN Gateway, however, the Inner VPN Gateway is not a perimeter VPN Gateway and, therefore, is not as exposed to external attacks, but it is more exposed to an internal attack.

In addition to performing the functions described in this Capability Package, an Inner VPN Gateway may also use AO/DAA-approved routing protocols on the Red network it is connected to. The Inner VPN Gateway cannot route packets between the Red and Gray networks; any packets received on a Red network interface and sent out a Gray network interface must be transmitted within an IPsec VPN tunnel configured according to this Capability Package.

5.3 CERTIFICATE AUTHORITIES

The CAs issue digital certificates for the VPN Gateways and VPN Clients in this solution. These certificates are used for authentication in establishing the IPsec tunnels between pairs of VPN Components. Given the architecture of the solution, there are distinct CAs for the Inner and Outer VPNs. The CA providing certificates for Inner VPN Components is located on the Red network, and the CA providing certificates for Outer VPN Components is located on the Gray Management network. This provides the key management separation required for two independent layers of encryption.

If the solution is supporting Red networks of different security levels, then a separate CA is needed for the Inner VPN Components of each security level.

If the organization has existing enterprise CAs that satisfy the requirements of this Capability Package, then those CAs may be used as part of the VPN solution rather than setting up new CAs dedicated to this solution.

5.4 Administration Workstations

Each VPN Gateway shall also have an Administration Workstation on the inside network that allows for maintaining, monitoring, and controlling all security functionality for the particular VPN Gateway. This Administration Workstation shall also allow for logging and configuration management, as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the Inner and Outer VPN Components. The Administration Workstation for the Inner VPN Components is located on the Red network, and the Administration Workstation for the Outer VPN Components is located on the Gray Management network, which shall not be directly connected to the Black or Red networks. This provides the separation necessary for two independent layers of protection.

If the solution is supporting Red networks of different security levels, then a separate Administration Workstation is needed for the Inner VPN Components of each security level.

If EUDs are remotely managed, then Administration Workstations are also responsible for remotely configuring and managing EUDs in accordance with this Capability Package. The Administration Workstation for Inner VPN Clients is located on the Red network, and the Administration Workstation for Outer VPN Clients is located on the Gray Management network.

5.5 End User Devices

EUDs are devices such as workstations, laptops, or tablets that a user directly interacts with and that implement their own VPN functionality, in whole or in part. There are two general types of EUD supported by the VPN solution: Local EUDs and Remote EUDs. Sections 5.5.1 and 5.5.2 describe the two types of EUD in more detail. Table 1 highlights the differences between the two types of EUD.

Table 1. Comparison between Local EUDs and Remote EUDs

Property	Local EUD	Remote EUD
Physical Operating Environment	Secure	Non-secure
Classification while Powered On	Same as Red Network	Same as Red Network
Classification while Powered Off	Same as Red Network	Unclassified but Controlled
Network it Directly Connects to	Black or Gray	Black
User Authentication to Red Services	Not Required	Required
Additional Technical Controls	Not Required	Required
User Agreement and Training	Not Required	Required

If an EUD is implemented on a Cross Domain Solution (CDS) approved by the AO/DAA, then the requirements specified in this Capability Package regarding EUDs only apply to the security domains within the CDS used to implement EUD functionality. In such an implementation, the CDS provides the necessary separation between EUD functionality and non-EUD functionality on the hardware platform. An EUD implemented on a CDS may have one or more security domains for EUD functionality (Inner VPN Client, Outer VPN Client, etc.) that are included in the solution boundary and one or more security domains that provide unrelated services and are not included in the solution boundary. As long as the AO/DAA-approved CDS isolates the security domains implementing EUD functionality from the other security domains, the EUD is able to comply with the requirements of this Capability Package.

5.5.1 Local End User Devices

A Local EUD is an EUD that is used exclusively within secure physical environments approved by the AO/DAA. Local EUDs are not subject to special physical handling restrictions beyond those applicable for classified devices, since they can rely on the environment they are in for physical protection. From the end user's perspective, they may be indistinguishable from devices connected directly to the Red network, especially if the VPN Clients are configured to automatically connect to the appropriate VPN Gateways. If the Local EUD physically connects directly to a Gray network, it only needs to implement an Inner VPN Client. If the Local EUD connects directly to a Black network, it needs to implement both an Inner VPN Client and an Outer VPN Client. (Appendix E provides examples of how an EUD may be designed to implement two VPN Clients.)

5.5.2 Remote End User Devices

A Remote EUD is an EUD that is used outside of a secure physical environment. Remote EUDs are subject to additional technical and operational security requirements, to compensate for the reduced level of physical security available.

To mitigate the risk to classified information if a Remote EUD is lost or stolen, the Remote EUD must be designed so that it becomes an unclassified device when powered off. This Capability Package offers two approaches to achieving this:

1) The Remote EUD can implement a data-at-rest solution that NSA has approved for the protection of information classified at the level of the Red network connected to the Remote EUD. Specification of such a data-at-rest solution is outside the scope of this Capability Package.

2) The Remote EUD can be designed to prevent any information retrieved from the Red network from being saved to any persistent storage media on the Remote EUD. Possible techniques for implementing this include, but are not limited to: using a thin client system configured not to allow data from the Red network to be saved on the Remote EUD, restricting the user to a non-persistent

virtual machine on the Remote EUD, and/or configuring the Remote EUD's operating system to prevent the user from saving data locally. Since the Remote EUD does not provide secure local storage for classified data, its user is also prohibited by policy from saving classified data to it. The Remote EUD in this case must also implement full disk encryption (FDE) compliant with FIPS 140-2, to protect the private keys stored on it from disclosure and to increase the difficulty of tampering with the software and configuration stored on it.

Either approach prevents any unprotected classified data from being stored on the Remote EUD once it is powered off.

After the VPN Clients on the Remote EUD authenticate themselves to the VPN Gateways they connect to, the user of the Remote EUD must authenticate himself or herself to the services on the Red network before gaining access to any classified data from them, via a user authentication mechanism approved by the AO/DAA. This mitigates the risk of a lost or stolen Remote EUD being used to connect to the Red network.

While powered on, the Remote EUD is classified at the same level of the Red network connected to the Remote EUD, since classified data may be present in volatile memory and/or displayed on screen. To mitigate the risk of accidental disclosure of classified information to unauthorized personnel while the Remote EUD is in use, the customer must define and implement an end user agreement for the Remote EUDs that specifies rules of use for the system. The customer must only grant users access to a Remote EUD after they agree to the end user agreement and receive training on how to use and protect their Remote EUD.

Remote EUDs can only directly connect to a Black network, and therefore need to implement both an Inner VPN Client and an Outer VPN Client. (Appendix E provides examples of how an EUD may be designed to implement two VPN Clients.)

5.5.3 PROVISIONING

Provisioning is the process through which EUDs (Local or Remote) are initialized before first use. During the provisioning process, the Security Administrator loads and configures the EUD's software. The Security Administrator also loads private keys and certificates obtained from the Certificate Authority Administrators (CAAs) onto the EUD. Provisioning is inherently an out-of-band process that requires physical access to the EUD.

If the solution owner is unable to remotely manage EUDs, they must be periodically re-provisioned in order to receive software and configuration updates. Re-provisioning consists of revoking the EUD's existing certificates and provisioning the EUD starting from a trusted baseline configuration, without making use of or retaining any data originally stored on the EUD.

Due to the time and effort needed to re-provision EUDs, it is preferable to remotely manage them when possible, in which case updated software and configuration data is provided from a central management site through the VPN solution to the EUD, after the EUD establishes the two IPsec tunnels (see Section 10.8).

5.5.4 INNER VPN CLIENTS

The Inner VPN Client is a component within all EUDs. The purpose of the Inner VPN Client is to establish an IPsec tunnel from the EUD to the Inner VPN Gateway. The tunnel can be configured to automatically be established as part of the EUD's power-on process, following establishment of the Outer VPN tunnel.

Remote administration is not a requirement of this Capability Package. However, if remote administration is implemented, the Inner VPN Client administration management will be performed over the Red network. Administrative data from the EUD must be protected as prescribed in this Capability Package.

5.5.5 OUTER VPN CLIENTS

The Outer VPN Client is a component within an EUD, and is only present on EUDs that directly connect to a Black network. The purpose of the Outer VPN Client is to establish an IPsec tunnel from the EUD to the Outer VPN Gateway in order to provide access to the Gray network. The tunnel can be configured to automatically be established as part of the EUD's power-on process.

Remote administration is not a requirement of this Capability Package. However, if remote administration is implemented, the Outer VPN Client administration management will be performed over the Gray Management network. Administrative data from the EUD must be protected as prescribed in this Capability Package.

5.6 GRAY NETWORK FIREWALLS

A VPN solution that supports multiple Red networks may include one or more Gray Network Firewalls, as described in Section 4.3.3.3. The primary purpose of a Gray Network Firewall is to block any packets sent between Inner VPN Components for Red networks of different classification levels. A Gray Network Firewall also blocks any packets sent between management components on the Gray network and Inner VPN Components for Red networks that operate at a classification level other than the highest classification level of data protected by the solution.

A Gray Network Firewall is a stateful traffic filtering device on the Gray network that restricts the flow of packets through it based at minimum on source and destination addresses, source and destination port numbers, and protocol identifiers. The set of filtering rules on the Gray Network Firewall is configured to allow only the set of data flows necessary for the solution to function as intended, and to deny all other traffic.

In order for the Gray Network Firewall to function effectively, the Gray network must use an addressing scheme that allows the Firewall to determine whether two devices on the network are allowed to send packets to one another based on their addresses. One possible approach would be to statically assign addresses for all devices connected to the Gray network, then define individual rules on the Gray Network Firewall to explicitly allow specific pairs of devices to send and receive packets on specific ports. To prevent address spoofing, the Gray Network Firewall also needs rules to restrict which source addresses are allowed to be accepted on which of the Firewall's physical network interfaces.

5.7 CRL Distribution Points

A CRL Distribution Point (CDP) is a server other than a CA that makes CRLs available to VPN Components within a solution. As described in Section 4.3.4, a VPN solution may use CDPs to provide CRLs to VPN Components before those VPN Components have established any VPN tunnels. For this to work, the CDPs are placed on the network reachable from the VPN Component's external interface: on the Black network for Outer VPN Components, and on the Gray network for Inner VPN Components.

A CDP is a web server whose sole function is to host copies of one or more CRLs for VPN Components to download before performing mutual authentication with one another during tunnel establishment. CDPs do not serve any other content, and in particular do not host any dynamically-generated content, nor do they provide any other services. Minimizing the attack surface is particularly important for an Outer CDP; since it is connected to the Black network, it is more exposed to external attack than most other components in the solution.

A CDP is located on a different network than the CA that issues the CRLs it hosts: an Outer CDP is on the Black network but hosts CRLs issued by the Gray CA, and an Inner CDP is on the Gray network but hosts CRLs issued by a Red CA. In order to copy new CRLs from a CA to a CDP, a one-way transfer mechanism is necessary. The transfer mechanism must be one-way, to prevent a return path from allowing malicious content to bypass a VPN Component and enter the Gray or Red network. The AO for the solution is given discretion to select a one-way transfer mechanism to use, which could be process-based (such as copying via write-once removable media) or technology-based (such as an approved cross-domain solution).

CDPs serve CRLs over unencrypted HTTP connections instead of TLS-encrypted HTTPS connections, because HTTPS would provide little additional security benefit and would reduce the robustness of the solution. A CRL contains the minimal set of information necessary to be used by the VPN Components, so there are few concerns with the confidentiality of the CRL's contents. A CRL's integrity is protected by the digital signature of the CA that issued it, so additional integrity protection in transit is unnecessary. Providing the CRLs over HTTPS would introduce a potential circular dependency: a VPN Component would need the CRL to determine whether the CDP's TLS certificate was revoked, but could not obtain the CRL until the CDP successfully authenticates itself to the VPN Component. Serving CRLs over ordinary HTTP follows the recommendation in RFC 5280 not to use HTTPS to distribute CRLs.

There may be multiple Inner CDPs or Outer CDPs within a solution. Additional CDPs provide redundancy should a CDP fail or become unavailable, since a VPN Component would only need to contact one of the CDPs in order to obtain the latest CRL.

CDPs may host delta CRLs in addition to complete CRLs. In large VPN solutions, the use of delta CRLs can reduce the amount of network traffic needed to distribute updated CRLs to each participating site.

This Capability Package does not require that CDPs be used within a solution, although it does levy requirements on any CDPs that are implemented. CDPs are expected to be used in large VPN solutions where manual, out-of-band CRL distribution is costly, difficult, or infeasible to achieve in a timely manner. CDPs allow CRLs to be distributed to large numbers of VPN Components in a mostly automated fashion.

5.8 Other Controls

There are additional controls that could be used within this solution to potentially reduce the overall risk.

First, a screening router can be used to filter packets from the Black network before they arrive at the Outer VPN Gateway and Outer CDP. The screening router could be part of the existing Black network, or could be added between the Outer VPN Gateway and existing Black network components. However, since the screening router would become part of the Black network, it is not considered to be part of the VPN solution itself.

Second, a more comprehensive Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) could be used if additional assurance is desired. In particular, a comprehensive IDS or IPS system on the Gray network could increase the difficulty of a rogue actor evading detection, since normal, legitimate traffic on the Gray network is relatively easy to characterize. However, an IDS or IPS on the Gray network would need to be standalone, as it would not be able to interconnect with similar systems on the Red or Black network.

Additionally, Auditors could monitor user connection metrics for anomalies and monitor individual user sessions. All monitoring of user sessions and metrics would be conducted from the Red network.

Finally, if an integrator is used for implementation of this solution, the customer can require separation of roles between individuals working on Red and Gray components. The separation of roles ensures that during the development of the solution no single individual can compromise Red and Gray components simultaneously.

6 KEY MANAGEMENT

One of the most difficult parts of any solution is determining how the key management will be implemented in a secure manner. In this solution, the only certificates necessary are for the device authentication certificates on each of the two VPN Components at the end of each IPsec tunnel. The certificates and private keys used in the solution are considered Controlled Unclassified Information (CUI), because they are only used for mutual device authentication, not for traffic encryption.

No single CA can provide keys to both the Inner and Outer VPN Components. The CA for the Outer VPN Components are located in the Gray Management network, connected to an Outer VPN Gateway. A Locally-run CA may need to be stood up to key the Outer VPN Components, requiring that a CA product be selected from the NSA-approved CSfC Component List for the Outer tunnel PKI. In addition, a Certificate Policy (CP)/Certification Practice Statement (CPS) document must be tailored in accordance with the AO/DAA from NSA Guidance for Key Management (KM) and Device Management (DM) when it becomes available on the CSfC website. The NSA Guidance for KM and DM provides the proper structure to implement the Key Management requirements of this Capability Package. Then it is the AO/DAA's responsibility to approve the use of this CA. If the Outer tunnel CA is an Enterprise CA already running on the Gray Management network, no additional approval is necessary for use of this CA.

The CA for the Inner VPN Components are located on the Red network, which may allow for use of existing Enterprise CAs already operational on the Red network, following the requirements in Section 10.10.2 of this Capability Package. For networks in which an existing Enterprise CA is not available, the use of a Locally-run CA on the Red network, following the requirements in Section 10.10.3, is an acceptable alternative. If the Inner tunnel CA is an Enterprise CA already running on the Red network, no additional approval is necessary for use of this CA. For example, a solution may use an Enterprise CA (such as a Committee on National Security Systems (CNSS)-approved CA, which follows Committee on National Security Systems Instruction (CNSSI) 1300 under the National Security Systems (NSS) PKI Root CA), to issue certificates to the Inner VPN Gateway. If, however, the Inner tunnel CA uses a Locally-run CA on the Red network, the approval process given in the preceding paragraph for the Outer tunnel CA applies and must be followed.

Each VPN Component has at least one CA signing certificate (sometimes referred to as a Trust Anchor), which is used by the VPN Component to authenticate to other VPN Components in the solution. If centralized management is used throughout the solution, there will be only one CA signing certificate in each VPN Component. Otherwise, one CA signing certificate is installed in each Inner VPN Component for each Inner Tunnel CA used in the system. Similarly, one CA signing certificate will be installed in each Outer VPN Component for each Outer Tunnel CA used in the system.

Each VPN Component will contain a private key that corresponds to a certificate issued by its CA, and one or more CA signing certificates as described above. Each VPN Gateway will also contain revocation information. The private key may be locally generated and must be adequately protected. Both Inner

and Outer tunnel PKIs should use Elliptic Curve Digital Signature Algorithm (ECDSA) signatures within X.509 certificates, but may use RSA2048 or DSA2048 prior to 1 October 2015. Any certificates using RSA2048 or DSA2048 must expire prior to 1 October 2015. The algorithms and elliptic curves that are approved for use in this VPN solution are found in Table 5 (see Section 10.2).

The VPN solution described here requires certificates to establish the secure tunnels between VPN Components. Without certificates, the network cannot function. Thus, an out-of-band method must be used to issue the initial certificates to the VPN Components. Future rekeying, however, should take place over the network through this solution prior to the current key's expiration. The key validity period for certificates issued by Locally-run CAs cannot exceed 14 months, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to Certificate Revocation Lists are distributed to VPN Gateways at within 24 hours of CRL issuance.

7 THREATS

This section details how the required components work together to provide overall security in the solution. Figure 2 through Figure 11 show the boundary of the VPN solution for each architecture variant covered by this Capability Package.

An assessment of security was conducted on each of the architectures described in this Capability Package while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data.

7.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the network without changing the state of the system. Threat actions include collecting or monitoring traffic (e.g., traffic analysis or sniffing the network) passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting the data in transit across the Black network is provided by the layered IPsec tunnels. To mitigate passive attacks, two layers of Suite B encryption, Advanced Encryption Standard (AES), are employed to provide confidentiality for the solution. Use of AES is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The two VPN Components that are used to set up the tunnels must be independent in a number of ways (see Section 9). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both tunnels.

The use of Remote EUDs to access classified information outside of a secure physical environment opens the possibility that an attacker with physical access to the Remote EUD's immediate environment could use surveillance techniques to obtain classified information without the user's knowledge while the Remote EUD is in use. The organization-defined user agreement tells users of Remote EUDs what measures they must follow when using and storing the Remote EUD to mitigate this threat.

The use of one or more Outer CDPs to distribute unencrypted CRLs on the Black network potentially allows a passive threat actor with access to the Black network path between the Outer CDP and Outer VPN Component to obtain a copy of the CRL issued by the Gray CA. However, the content of the CRL is primarily limited to a list of serial numbers of revoked certificates, the date and time when each certificate was revoked, and a high-level reason why each certificate was revoked (such as key compromise or cessation of operation). The CRL does not specify what certificates are still valid, nor does it identify the physical or network locations of any components in the solution. The CRL also does not reveal any information about certificates issued by anything other than the Gray CA. If a solution owner's AO/DAA considers the limited information in a CRL too sensitive to distribute on the Black network, the solution owner can choose not to implement Outer CDPs and rely on other means to distribute CRLs to Outer VPN Components in a timely fashion.

7.2 External (Active) Threats

This threat refers to outsiders gaining unauthorized access to a system or network, exfiltration of sensitive Red network data, or degradation of availability of the system or network. Threat actions include introducing viruses, malware, or worms with the intention to compromise the network or exfiltrate data, or to analyze the architecture of the network or system for future attacks. Adversaries could gain access to a VPN Gateway or EUD, and then exploit or compromise other devices on the network. Denial of Service (DoS) or Distributed DoS (DDoS) attacks compromise availability of the system, degrading/disrupting secure communication across the Black network. Further external threat actions would include social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

7.2.1 Rogue Traffic

One method for detecting rogue traffic from an external attack as it attempts to pass through one or both VPN Components is by having the port filtering native to each VPN Gateway enabled and configured to audit and log any traffic that is not of the format described in the configuration (see Section 10.9). It is required that the port filtering be set up to block: 1) any traffic not coming from or going to an IP address on the network at the other site, 2) traffic not contained in IP packets other than control plane protocols needed for network operation and approved by AO/DAA policy, and 3) traffic going to unexpected ports. This will allow the Auditor(s) and/or the Security Administrator(s) (see

Section 12) to detect whether the Outer VPN Gateway has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of misconfigured Outer VPN Gateways.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on the Red and Gray Management networks to ensure the VPN Gateway configurations are not changed without the knowledge of the Auditor and Security Administrator. The Auditor also ensures through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of VPN Gateway misconfigurations.

Remote EUDs are protected from rogue traffic through the use of traffic filtering rules configured on its interfaces connected to the Black network to drop any traffic not necessary for connecting to the Outer VPN Gateway. Appendix E provides additional guidance for how packet filtering may be implemented on the EUD.

CDPs are protected from rogue traffic by implementing port filtering on the server. Rogue traffic to CDPs can be further mitigated by implementing a firewall or other packet filtering device between the CDP and the rest of the network.

7.2.2 Malware and Untrusted Updates

The Administration Workstations and CAs for the Red network shall be distinct from the Administration Workstations and CAs for the Gray network. This separation will minimize the potential of malware on a single device impacting components supporting both the Inner and Outer VPN tunnels.

Each individual component of this solution has the capability to perform trusted updates through verification of a signature or hash to ensure that the update is from a reliable source, such as signed by the vendor. This mitigates threats of malicious users trying to push updates or code patches that affect the security of the component (and therefore system). The source of all updates and patches should be verified before installation occurs.

7.2.3 Denial of Service

DoS attack risks cannot be completely mitigated. The solution requires dropping all packets that are not Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), or other approved protocols on the appropriate interfaces, which significantly reduces the potential of flooding attacks. For customers that require more protection against these attacks, one option is the use of an optional perimeter router to perform additional filtering. This moves the responsibility to protect against a DoS attack away from this solution and back to a router that is already an established part of the customer's network. Another option for customers requiring more protection is to add additional filtering based on specifics like known network IP addresses to filter traffic from devices not included in this solution, although the feasibility of doing so for Remote EUDs is limited unless the entire set of IP addresses the Remote EUDs

could be assigned is known. Other mitigations are acceptable and up to the AO/DAA to approve their use.

A single component failure is likely to result in a DoS condition. One assumption underlying this solution is that high assurance of availability is not required. If availability is critical for the customer, network redundancy can support further DoS protection as well as having procedures for response when loss of availability is detected.

When using Outer CDPs to distribute CRLs to Outer VPN Components on the Black network, a sustained DoS attack on the CDPs could prevent Outer VPN Components from receiving updated CRLs. If the CRLs cached at the Other VPN Components then expire, they would be unable to establish VPN connections due to the inability to check the revocation status of certificates during the mutual authentication process. Deploying multiple Outer CDPs reduces the likelihood of a successful DoS attack on this part of the solution, since as long as even one Outer CDP is available, Outer VPN Components will be able to retrieve CRL updates. Additionally, a solution using CDPs should still have procedures in place for out-of-band CRL distribution, to use in the event that all Outer CDPs become unavailable.

7.2.4 Social Engineering

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in this section and already discussed.

7.3 Insider Threats

This threat refers to an authorized or cleared person or group of people with access, physical or logical, to the network or system who may act maliciously or negligently, resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the equipment, dishonest employees, or those that have the means and desire to gain escalated privileges on the network.

Threat actions include insertion or omission of data entries that result in loss of data integrity, unintentional access to an unauthorized system or network, willingly changing the configuration of an EUD, unwillingly or unknowingly executing a virus or malware, intentionally exposing the network and systems to viruses or malware, cross-contaminating a system or network with data from a higher classification to a lower classification (e.g., Secret data to Unclassified network or system), or malicious or unintentional exfiltration of classified data. Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 12). In addition, logging and auditing of security critical functionality (see Section 10.9) is required. Also, strong

authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. Finally, outbound filters on the VPN Gateways and EUDs are configured to look for traffic leaving the internal network that does not go through the IPsec tunnels. In scenarios that need additional assurance, an optional IDS could be deployed on the Gray network to help identify whether there is a failure, misconfiguration, or attack on the Inner or Outer VPN Gateways.

The use of Remote EUDs can make detection of malicious users more difficult since the only available means of monitoring Remote Users' behavior is to monitor their network activity. In order to mitigate this threat, an organization can implement monitoring of the Remote Users. Additionally, organizations concerned about users misbehaving when connected remotely may wish to restrict the use of Remote EUDs to those deemed sufficiently trustworthy.

7.4 Supply Chain Threats

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the information and communication technology (ICT) components embedded in the systems and networks upon which the ability to perform their missions rely. The supply chain for those ICT components are the underpinnings of those systems and networks and supply chain attacks are attempts to proactively compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component; they are only able to provide assurances based on their reliance of established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify and test, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine the source where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA-approved Product Supply Chain Threat Assessment process (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance).

There are doctrinal requirements placed on Product Selection, Implementers, and System Integrators of these solutions to minimize the threat of supply chain attacks (see Sections 9, 11, and 12).

7.5 INTEGRATOR THREATS

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different than a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures.

In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the VPN solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution.

8 VPN SOLUTION ARCHITECTURE AND CONFIGURATION REQUIREMENTS

The following five sections (Sections 9 through 13) specify requirements for implementations of VPN solutions compliant with this Capability Package. Although most requirements are applicable to all compliant implementations, some requirements are only applicable to implementations whose architectures implement certain features. For example, requirements dealing with EUDs do not apply to implementations that do not include EUDs. Table 2 lists the architecture variants covered by this Capability Package and the designators used in the requirements tables to refer to each.

Table 2. Architecture Designators

Architecture	Designator	Description
Multiple Sites	M	VPN solution architectures that interconnect two or more sites, as described in Sections 4.3.1 and 4.3.3.
Remote EUDs	R	VPN solution architectures that include Remote EUDs, as described in Sections 4.3.2 and 5.5.2.
Local EUDs	L	VPN solution architectures that include Local EUDs, as described in Sections 4.3.2 and 5.5.1.

Architecture	Designator	Description
Gray Network Firewalls	F	VPN solution architectures that include Gray Network Firewalls, as described in Sections 4.3.3.3 and 5.6. This architecture cannot be implemented without also implementing architecture M, R, and/or L.
CDPs	C	VPN solution architectures that include CDPs, as described in Sections 4.3.4 and 5.7. This architecture cannot be implemented without also implementing architecture M, R, and/or L.

The Capability Package includes two categories of requirements specified based on the below guidance:

- An Objective (O) requirement specifies a feature or function that is desired or expected. Organizations should implement objective requirements in lieu of the corresponding Threshold requirement where feasible.
- A Threshold (T) requirement specifies a minimum acceptable feature or function that still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to system maturity). A solution implementation must satisfy all applicable Threshold requirements, or their corresponding Objective requirements, in order to comply with this Capability Package.

In many cases, the Threshold requirement also serves as the Objective requirement (T=O). Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement improves upon the Threshold requirement and may replace the Threshold requirement in future versions of this Capability Package.

In order to comply with this Capability Package, a solution must at minimum implement all Threshold requirements (or their corresponding Objective requirements) associated with each of the architectures it supports. Solutions should implement the Objective requirements associated with those architectures where feasible. Each row in the requirements tables in the following five sections includes a comma-separated list of architectures to which the requirement applies. For example, a VPN solution interconnecting two or more sites that also includes Local EUDs must implement the Threshold requirements for Multiple Sites (M) and the Threshold requirements for Local EUDs (L), but it does not need to implement the Threshold requirements that apply solely to Remote EUDs (R). In some cases, a requirement only applies to solutions that implement two architectures together. In this case, a plus sign (+) is used to designate the combination of two architectures. For example, a requirement designated as F+C applies only to solution that implement *both* Gray Network Firewalls *and* CDPs, but not to solutions that only implement one or the other.

9 GUIDELINES FOR SELECTING COMPONENT PRODUCTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 3. Product Selection Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-PS-1	The products used for the Inner and Outer VPN Gateways shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	M, R, L	T=O
VPN-PS-2	The products used for the Inner and Outer VPN Clients shall be chosen from the list of IPsec VPN Clients on the CSfC Components List.	R, L	T=O
VPN-PS-3	The products used for the Inner tunnel and Outer tunnel CAs either shall be chosen from the list of CAs on the CSfC Components List or shall be Enterprise CAs.	M, R, L	T=O
VPN-PS-4	The Inner and Outer VPN Gateways shall come from different vendors. One vendor cannot be a subsidiary of the other.	M, R, L	T=O
VPN-PS-5	The Inner and Outer VPN Gateways shall be logically separated using an NSA-approved mechanism.	M, R, L	T
VPN-PS-6	The Inner and Outer VPN Gateways shall be run on physically separate hardware.	M, R, L	O
VPN-PS-7	The Inner and Outer VPN Gateways shall not use the same OS for critical IA security functionality. Differences between Service Packs (SP) or version numbers for a particular vendor's OS do not provide adequate diversity.	M, R, L	T=O
VPN-PS-8	The Outer tunnel CA shall come from a different vendor than the CA used by the Inner tunnel.	M, R, L	O
VPN-PS-9	The Inner and Outer VPN Clients shall come from different vendors. One vendor cannot be a subsidiary of the other.	R, L	T=O
VPN-PS-10	The cryptographic libraries used by the Inner and Outer VPN Gateways shall be different independent implementations from different vendors.	M, R, L	O
VPN-PS-11	The cryptographic libraries used by the Inner and Outer VPN Clients shall be different independent implementations from different vendors.	R, L	O
VPN-PS-12	The cryptographic libraries used by the Inner and Outer Certificate Authorities shall be different independent implementations from different vendors.	M, R, L	O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-PS-13	Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA approved Product Supply Chain Threat Assessment process. (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance.)	M, R, L	T=O
VPN-PS-14	The Gray Network Firewalls and Inner VPN Gateways shall belong to different product families.	F	T
VPN-PS-15	The Gray Network Firewalls and Inner VPN Gateways shall come from different vendors. One vendor cannot be a subsidiary of the other.	F	O
VPN-PS-16	The products used for the Gray Network Firewalls shall be chosen from the list of Firewalls on the CSfC Components List.	F	T=O

It is preferred that the CAs be part of a customer's enterprise keying solution. In that case, the CA will not be selected from the CSfC Components List because it already exists on the Red or Gray network. If there is no existing Enterprise CA, however, the CA must also be selected from the CSfC Components List.

10 CONFIGURATION

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the VPN solution.

10.1 Overall Solution Requirements

Table 4. Overall Solution Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-SR-1	The Gray Management network traffic shall be physically or cryptographically separate from the data traffic on the Gray network (see Section 4.1.2).	M, R, L	T=O
VPN-SR-2	Fundamental network architecture components, such as DNS and NTP that are not explicitly included in the solution, shall be located on the inside network (i.e., Gray network for Outer VPN Components and Red network for Inner VPN Components; see Section 4.7).	M, R, L	O
VPN-SR-3	Sites that need to communicate shall ensure that the VPN Gateways selected by each site are interoperable (see Section 4.2).	M	T=O
VPN-SR-4	The time of day on the Inner VPN Gateways and each component within the Red network shall be synchronized with the same time source located in the Red network.	M, R, L	T=O
VPN-SR-5	The time of day on the Outer VPN Gateways and each component within the Gray network shall be synchronized with the same time source located in the Gray Management network.	M, R, L	T=O
VPN-SR-6	The VPN clients selected for EUDs shall be interoperable with the corresponding VPN Gateways.	R, L	T=O
VPN-SR-7	Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed.	M, R, L	T=O
VPN-SR-8	All components shall be properly configured according to local policy and U.S. Government guidance (e.g., DISA gold disk, NSA guidelines).	M, R, L	T=O

10.2 Configuration Requirements for All VPN Components

Table 5. Approved Suite B Algorithms

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
Overall Level of Security	128 bits	192 bits	
Confidentiality (Encryption)	AES-128	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature)	ECDSA over the curve P-256 with SHA-256	ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-3 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
	RSA 2048 (prior to 1 October 2015)	N/A	FIPS PUB 186-3
	DSA 2048 (prior to 1 October 2015)	N/A	FIPS PUB 186-3
Key Exchange/ Establishment	ECDH over the curve P-256 (DH Group 19)	ECDH over the curve P-384 (DH Group 20)	NIST SP 800-56A IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
	DH 2048 (prior to 1 October 2015)	N/A	NIST SP 800-56A
Integrity (Hashing)	SHA-256	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Can protect	Up to Secret	Up to Top Secret	

Table 6. Configuration Requirements for Both VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-CR-1	The proposals offered by VPN Components in the course of establishing the IKE Security Association (SA) and the ESP SA for the Inner and Outer Tunnels shall be configured to offer algorithm suite(s) containing only Suite B algorithms (see Table 5).	M, R, L	T=O
VPN-CR-2	*Moved to VPN-PF-10*		

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-CR-3	The default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Components shall not be used for establishing SAs.	M, R, L	T
VPN-CR-4	The default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Components shall be removed.	M, R, L	O
VPN-CR-5	A unique device certificate shall be loaded onto each VPN Component along with the corresponding CA (signing) certificate.	M, R, L	T=O
VPN-CR-6	The device certificate shall be used for VPN Component authentication during IKE.	M, R, L	T=O
VPN-CR-7	VPN Gateway authentication shall include a check that the certificate is authorized which can include a Certificate Revocation List (CRL) or whitelist.	M, R, L	T=O
VPN-CR-8	VPN Component authentication shall include a check that the certificate is not expired.	M, R, L	T=O
VPN-CR-9	VPN Gateways shall not output or transmit their stored private keys.	M, R, L	T=O
VPN-CR-10	The only approved physical paths leaving the Red network shall be through a VPN solution in accordance with this Capability Package or via an NSA-approved solution for protecting data in transit.[1]	M, R, L	T=O
VPN-CR-11	One IPsec tunnel shall use IKEv2 (RFC 5996) key exchange and the other shall use IKEv1 (RFC 2409) key exchange in Main Mode on Phase 1.	M, R, L	T
VPN-CR-12	Both IPsec tunnels shall use IKEv2 (RFC 5996) key exchange.	M, R, L	O
VPN-CR-13	*Moved to VPN-PF-11*		
VPN-CR-14	VPN Components shall store and output passwords in cryptographically protected formats only.	M, R, L	T=O
VPN-CR-15	The Inner VPN Components shall use protocols and algorithms for creating inner VPN tunnels selected from Table 5 that are approved to protect the highest classification level of the Red network data.	M, R, L	T
VPN-CR-16	The Outer VPN Components shall use protocols and algorithms for creating outer VPN tunnels selected from Table 5 that are approved to protect the highest classification level of the Red network data.	M, R, L	T

[1] In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) equipment. In particular, it is okay for a given site to have both an egress path via an NSA-certified device and an egress path via a layered COTS solution conforming to this Capability Package. This will allow a site to communicate with remote sites that use either solution.

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-CR-17	The VPN Components shall use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite 2 in Table 5.	M, R, L	O
VPN-CR-18	The VPN Components shall use Cipher Block Chaining for IKE encryption.	M, R, L	T=O
VPN-CR-19	The VPN Components shall use Cipher Block Chaining for ESP Encryption.	M, R, L	T
VPN-CR-20	The VPN Components shall use Galois Counter Mode for ESP Encryption.	M, R, L	O
VPN-CR-21	The VPN Components shall set the IKE SA lifetime to at most 24 hours.	M, R, L	T=O
VPN-CR-22	The VPN Components shall set the ESP SA lifetime to at most 8 hours.	M, R, L	T=O
VPN-CR-23	Inner VPN Gateways shall only authenticate and establish an IPsec tunnel with one another if their Red networks operate at the same security level (as defined in this Capability Package).	M	T=O
VPN-CR-24	An Inner VPN Gateway and Inner VPN Client shall only authenticate and establish an IPsec tunnel with one another if the Inner VPN Client's EUD operates at the same security level (as defined in this Capability Package) as the Inner VPN Gateway's Red network.	R, L	T=O
VPN-CR-25	The VPN Components shall reauthenticate the identity of the VPN Component at the other end before rekeying the IKE SA.	M, R, L	T=O

10.3 Additional Requirements for Inner VPN Components

Table 7. Additional Requirements for Inner VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-IR-1	The Inner VPN component shall use Tunnel mode IPsec or Transport mode IPsec with an associated IP tunneling protocol (e.g., GRE).	M, R, L	T=O
VPN-IR-2	The packet size for packets leaving the external interface of the Inner VPN component shall be configured to keep the packets from being fragmented and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4) or Path MTU (PMTU) (for IPv6) and should consider the Black network and Outer VPN component MTU/PMTU values to achieve this.	M, R, L	O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-IR-3	The Inner VPN Gateway shall encrypt all traffic originating in the Red network before it goes out the external interface towards the Outer VPN Gateway in accordance with this Capability Package.	M, R, L	T=O
VPN-IR-4	The Inner VPN Client of EUDs shall encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g. DHCP) and locate the VPN Gateway (e.g. DNS lookup of the VPN Gateway's IP address), in accordance with this Capability Package.	R, L	T=O

10.4 Additional Requirements for Outer VPN Components

Table 8. Additional Requirements for Outer VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-OR-1	The Outer VPN Component shall use Tunnel mode IPsec.	M, R, L	T=O
VPN-OR-2	The Outer VPN Gateway shall encrypt all traffic originating in the Red or Gray networks before it goes out the external interface in accordance with this Capability Package.	M, R, L	T=O
VPN-OR-3	All traffic received by the Outer VPN Gateway, with the exception of Control Plane traffic, shall have already been encrypted once in accordance with VPN-IR-3, VPN-IR-4, or VPN-RA-1.	M, R, L	T=O
VPN-OR-4	The Outer VPN Client of EUDs shall encrypt all traffic, with the exception of traffic necessary for the EUD to connect to the physical network (e.g. DHCP) and locate the VPN Gateway (e.g. DNS lookup of the VPN Gateway's IP address), in accordance with this Capability Package.	R, L	T=O
VPN-OR-5	All traffic originating from the EUD, with the exception of traffic necessary for the EUD to connect to the physical network (e.g. DHCP) and locate the VPN Gateway (e.g. DNS lookup of the VPN Gateway's IP address), shall have already been encrypted once by the Inner VPN client in accordance with VPN-IR-4.	R, L	T=O
VPN-OR-6	If one or more virtual machines are used on the EUD to separate the Inner and Outer VPN Clients, then the Outer VPN Client shall not run on the host operating system.	R, L	T=O

10.5 Requirements for End User Devices

Table 9. Requirements for End User Devices

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-EU-1	Remote EUDs shall either implement an NSA-approved data-at-rest (DAR) solution or prohibit local user storage of information retrieved from the Red network (see Section 5.5.2).	R	T=O
VPN-EU-2	Remote EUDs shall implement FIPS-140-2 (or later) compliant FDE or a NSA-approved DAR solution.	R	T=O
VPN-EU-3	EUDs shall permit only Security Administrators to use external data storage media (e.g. USB storage devices, DVDs).	R, L	T=O
VPN-EU-4	On EUDs that directly connect to a Black network, the Inner and Outer VPN Clients on the EUD shall use separate private key stores.	R, L	T=O
VPN-EU-5	On EUDs that directly connect to a Black network, the Inner and Outer VPN Clients on the EUD shall be implemented on separate IP stacks.	R, L	T=O
VPN-EU-6	The EUDs shall be provisioned within a physical environment certified to protect the highest classification level of the Red network.	R, L	T=O
VPN-EU-7	If the EUD is not remotely administered, then it shall only be updated and rekeyed through re-provisioning.	R, L	T=O
VPN-EU-8	Rekeying of the EUDs shall be done prior to expiration of keys.	R, L	T
VPN-EU-9	Rekeying of the EUDs shall be done over the VPN solution network prior to expiration of keys.	R, L	O
VPN-EU-10	The EUD shall be re-provisioned if there is any reason to believe it has been compromised.	R, L	T=O
VPN-EU-11	Remote Users shall successfully authenticate themselves to the services they access on the Red network.	R	T=O
VPN-EU-12	Red network services shall not transmit any classified data to Remote EUDs until user authentication succeeds.	R	T=O
VPN-EU-13	EUDs shall implement the BIOS security guidelines specified in NIST SP 800-147.	R, L	O
VPN-EU-14	All Remote Users shall sign an organization-defined user agreement before being authorized to use a Remote EUD.	R	T=O
VPN-EU-15	All Remote Users shall receive an organization-developed training course for operating a Remote EUD prior to use.	R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-EU-16	At a minimum, the organization defined user agreement shall include each of the following: • Consent to monitoring • OPSEC guidance • Required physical protections to employ when operating and storing the Remote EUD • Restrictions for when and where the Remote EUD may be used • Verification of IA Training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities	R	T=O
VPN-EU-17	EUDs shall generate logs and send to a central log server in the Red network.	R, L	O
VPN-EU-18	EUDs shall be dedicated for use solely in the VPN solution.	R, L	T=O

10.6 Port Filtering Requirements for VPN Components

Table 10. Port Filtering Requirements for VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-PF-1	For all interfaces connected to a Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed shall be blocked.	M, R, L	T=O
VPN-PF-2	For all interfaces connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and management and control plane protocols (as defined in this Capability Package) approved by policy are allowed. All packets not explicitly allowed shall be blocked.	M, R, L	T=O
VPN-PF-3	Traffic filtering rules on the VPN Gateways shall be applied based on known VPN Gateway addresses or address ranges to further protect against unknown IPsec traffic.	M	T=O
VPN-PF-4	Traffic filtering rules on the VPN Gateways shall be applied based on known EUD addresses or address ranges to further protect against unknown IPsec traffic.	R, L	O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-PF-5	Traffic filtering rules on the EUD shall be applied based on known VPN Gateway addresses or address ranges to further protect against unknown IPsec traffic.	R, L	T=O
VPN-PF-6	Any service or feature that allows the Outer VPN Component or the EUD to contact a third party server (such as one maintained by the manufacturer) shall be blocked.	M, R, L	T
VPN-PF-7	Any service or feature that allows the Outer VPN Component or the EUD to contact a third party server (such as one maintained by the manufacturer) shall be disabled.	M, R, L	O
VPN-PF-8	Outer VPN Gateways shall block all data (by ports and IP addresses) on their Gray Management network interface that is not necessary for the management of Outer VPN Gateways.	M, R, L	T=O
VPN-PF-9	Multicast messages received on external interfaces of Outer VPN Components shall be dropped.	M, R, L	T=O
VPN-PF-10	The VPN Components shall be configured to restrict the IP address range for the network Administration Workstation to the smallest range possible	M, R, L	T=O
VPN-PF-11	For solutions using IPv4, each VPN Component shall drop all packets that use IP options.	M, R, L	T=O
VPN-PF-12	For solutions using IPv4, each VPN Component shall only accept packets with TCP, UDP or ICMP in the IPv4 Protocol field and drop all other packets.	M, R, L	T=O
VPN-PF-13	For solutions using IPv6, each VPN Component shall only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets.	M, R, L	T=O
VPN-PF-14	The internal interfaces of the Outer VPN Gateways shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	M, R, L	T=O

10.7 Configuration Change Detection Requirements

Table 11. Configuration Change Detection Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-CM-1	A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor.	M, R, L	T=O
VPN-CM-2	An automated process shall ensure that configuration changes are logged.	M, R, L	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-CM-3	Log messages generated for configuration changes shall include the specific changes made to the configuration.	M, R, L	T=O

10.8 Requirements for VPN Component Administration

Only authorized Security Administrators will be allowed to administer the VPN Components. The VPN solution will be used as transport for the SSHv2, IPsec, or TLS data from the Administration Workstation to the VPN Component. This means that to remotely administer an Outer VPN component, the existing tunnel between Outer VPN components will carry the SSH, IPsec, or TLS data and in order to remotely administer an Inner VPN Component, the SSH, IPsec, or TLS data will travel inside the two tunnels to reach the remote Inner VPN Component.

Table 12. Requirements for VPN Component Administration

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-RA-1	All administration performed over a network connection shall be done using SSHv2, IPsec, or TLS.	M, R, L	T=O
VPN-RA-2	EUDs shall be remotely administered.	R, L	O
VPN-RA-3	If SSHv2 is utilized for component administration, the protocol shall be implemented as specified in RFCs 4252-4254 and 6239.	M, R, L	T=O
VPN-RA-4	If IPsec is utilized for component administration, the protocol shall be implemented as specified in RFCs 2409, 4302, 4303, 4307, 4308, 5996, 6379, and 6380.	M, R, L	T=O
VPN-RA-5	If TLS is utilized for component administration, the protocol shall be implemented as specified in RFCs 5246 and 6460.	M, R, L	T=O
VPN-RA-6	The Administration Workstations shall be dedicated for the purposes given in Section 5.4.	M, R, L	T=O
VPN-RA-7	Antivirus software shall be running on all Administration Workstations.	M, R, L	T=O
VPN-RA-8	Security Administrators shall authenticate to solution components before performing administrative functions.	M, R, L	T
VPN-RA-9	Security Administrators shall authenticate to solution components with Suite B compliant certificates (see Table 5) before performing administrative functions.	M, R, L	O

10.9 AUDITING REQUIREMENTS

Table 13. Auditing Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-AU-1	Each VPN Gateway shall log when a VPN tunnel is established.	M, R, L	T=O
VPN-AU-2	Each VPN Gateway shall log when a VPN tunnel is terminated.	M, R, L	T=O
VPN-AU-3	All actions performed on the audit log (off-loading, deletion, etc.) shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-4	All actions involving identification and authentication shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-5	Attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-6	All actions performed by a user with super privileges shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-7	Any escalation of user privileges shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-8	Certificate operations including generation, loading, or revoking of certificates shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-9	Changes to time shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-10	Receipt of unexpected data on Gray data or management network interfaces shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-11	Logs shall be monitored by the Auditor on at least a weekly basis.	M, R, L	T=O
VPN-AU-12	All built-in self-test results, which may indicate failures in cryptographic functionality, shall be logged on a continuous basis.	M, R, L	T=O
VPN-AU-13	The set of auditable events specified in the CPS shall be monitored and logged within the outer-tunnel CAs used for VPN Gateways on a continuous basis when in use.	M, R, L	T=O
VPN-AU-14	Each audit event entry shall record the date and time of the event and identify the time zone offset.	M, R, L	T=O
VPN-AU-15	Each audit event entry shall include the identifier of the event.	M, R, L	T=O
VPN-AU-16	Each audit event entry shall record the type of event.	M, R, L	T=O
VPN-AU-17	Each audit event entry shall record the success or failure of the event to include failure code, when available.	M, R, L	T=O
VPN-AU-18	Each audit event entry shall record the subject identity.	M, R, L	T=O
VPN-AU-19	Each audit event entry shall record the source address for network based events.	M, R, L	T=O
VPN-AU-20	Each audit event entry shall record the user and role identification for role based events.	M, R, L	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-AU-21	Auditors shall detect when two or more simultaneous VPN connections from different IP addresses are established using the same device certificate.	M, R, L	O
VPN-AU-22	Upon notification of two or more simultaneous VPN connections from different IP addresses using the same device certificate, the Certificate Authority Administrator shall revoke the device certificate and provide an updated Certificate Revocation List (CRL) to the Security Administrator.	M, R, L	O
VPN-AU-23	The Security Administrator shall immediately drop the session upon notification of two or more simultaneous VPN connections from different IP addresses using the same device certificate.	M, R, L	O
VPN-AU-24	Event logs from components managed via the Red networks shall be forwarded to a centralized host for analysis.	M, R, L	O
VPN-AU-25	Event logs from components managed via the Gray Management network shall be forwarded to a centralized host for analysis.	M, R, L	O
VPN-AU-26	VPN Components shall log the failure to download the CRL from the Inner or Outer CDP.	C	T=O
VPN-AU-27	VPN Components shall log if the version of the CRL downloaded from the Inner or Outer CDP is older than the current cached CRL.	C	T=O
VPN-AU-28	VPN Components shall log if signature validation of the CRL downloaded from the Inner or Outer CDP fails.	C	T=O
VPN-AU-29	Gray Network Firewalls shall log whenever a packet is denied.	F	T=O

10.10 Key Management Requirements

10.10.1 PKI Requirements for VPN Components

Table 14. PKI Requirements for VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-KM-1	The key sizes and algorithms used for the Inner and Outer VPN Components shall be as specified in Table 5.	M, R, L	T=O
VPN-KM-2	The CA supporting the Inner VPN Components shall be physically separate from the CA supporting the Outer VPN Components.	M, R, L	T=O
VPN-KM-3	Both the Inner and Outer tunnel CAs shall operate under a CPS that is formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.	M, R, L	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-KM-4	Both Inner and Outer tunnel CAs shall use RSA2048 or DSA2048 within X.509 version 3 certificates.	M, R, L	T
VPN-KM-5	Any certificates using RSA2048 or DSA2048 shall expire prior to 1 October 2015.	M, R, L	T
VPN-KM-6	Both Inner and Outer tunnel CAs shall use ECDSA signatures within X.509 version 3 certificates.	M, R, L	O
VPN-KM-7	Inner VPN Components shall only trust an Inner tunnel CA used within the solution.	M, R, L	T=O
VPN-KM-8	Outer VPN Components shall only trust an Outer tunnel CA used within the solution.	M, R, L	T=O
VPN-KM-9	All public/private key pairs and certificates for VPN Components shall be used for authentication only.	M, R, L	T=O
VPN-KM-10	VPN Component keys shall not be escrowed.	M, R, L	T=O
VPN-KM-11	The VPN Gateways shall be initially keyed within a physical environment certified to protect the highest classification level of the VPN solution network.	M, R, L	T=O
VPN-KM-12	Rekeying of the VPN Gateways shall be done prior to expiration of keys.	M, R, L	T=O
VPN-KM-13	*Superseded by VPN-KM-26*		
VPN-KM-14	If rekeying of the VPN Gateways is not completed prior to expiration of keys, they shall be rekeyed through the same process as initial keying.	M, R, L	T=O
VPN-KM-15	Certificate revocation information shall be made available by posting the data to a repository or service that is available for the VPN Components.	M, R, L	T=O
VPN-KM-16	New certificates shall be issued as needed in accordance with local policy.	M, R, L	T=O
VPN-KM-25	CAs shall issue an updated CRL within 1 hour of a certificate revocation.	M, R, L	T=O
VPN-KM-26	When a new CRL is issued, the updated CRL shall be distributed to the VPN Gateways within 24 hours.	M, R, L	T=O
VPN-KM-27	CRLs shall expire no later than 31 days after their issue date.	M, R, L	T=O
VPN-KM-28	Certificate Revocation Lists (CRLs) shall comply with RFC 5280.	M, R, L	T=O

10.10.2 ENTERPRISE PKI REQUIREMENTS

Table 15. Enterprise PKI Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-KM-17	Enterprise CAs shall assert a registered Object Identifier (OID) to all of its VPN Components.	M, R, L	O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-KM-18	Enterprise CAs shall be located on the Red network for Inner VPN Components and on the Gray network for Outer VPN Components, and be approved to issue certificates (such as one that follows CNSSI 1300 under the NSS PKI Root CA).	M, R, L	T=O

10.10.3 LOCALLY-RUN PKI REQUIREMENTS

Table 16. Locally-Run PKI Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-KM-19	The key validity period for certificates issued by Locally-run CAs shall not exceed 14 months.	M, R, L	T=O
VPN-KM-20	Locally-run CAs shall assert a registered OID to all of its VPN Components.	M, R, L	T=O
VPN-KM-21	Locally-run Red network CAs shall only issue certificates to Inner VPN Components of CSfC Solutions or to support its own operation.	M, R, L	T=O
VPN-KM-22	Locally-run Gray network CAs shall only issue certificates to Outer VPN Components of CSfC Solutions or to support its own operation.	M, R, L	T=O
VPN-KM-23	Locally-run CAs shall have a limited name space to issue certificates.	M, R, L	T=O
VPN-KM-24	Locally-run CAs shall issue certificates with unique names.	M, R, L	T=O

10.11 GRAY NETWORK FIREWALL REQUIREMENTS

Table 17. Gray Network Firewall Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-FW-1	Gray Network Firewalls shall permit Internet Key Exchange (IKE) and Internet Protocol Security (IPsec) traffic between the two Inner VPN Components protecting networks of the same classification level.	F	T=O
VPN-FW-2	Gray Network Firewalls shall allow HTTP traffic between Inner VPN Gateways and Inner CDPs.	F+C	T
VPN-FW-3	Gray Network Firewalls shall allow HTTP GET requests from Inner VPN Components to an Inner CDPs for the URL of the CRL needed by the Inner VPN Component, and block all other HTTP requests.	F+C	O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-FW-4	Gray Network Firewalls shall allow HTTP responses from Inner CDPs to Inner VPN Components that contain a well-formed CRL per RFC 5280, and block all other HTTP responses.	F+C	O
VPN-FW-5	Gray Network Firewalls shall only accept management traffic on the physical ports connected to the Gray Management Network.	F	T=O
VPN-FW-6	Gray Network Firewalls shall only permit packets whose source and destination IP addresses match the external interfaces of the Inner VPN Components communicating at the same classification level.	F	T=O
VPN-FW-7	Gray Network Firewalls shall be physically separate from Inner VPN Gateways.	F	T=O
VPN-FW-8	Gray Network Firewalls shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	F	T=O
VPN-FW-9	Gray Network Firewalls shall deny all traffic that is not explicitly allowed by requirements VPN-FW-1, VPN-FW-2, VPN-FW-3, VPN-FW-4, or VPN-FW-5.	F	T=O
VPN-FW-10	All physical paths within the Gray network between two Inner VPN Components for Red networks of different classification levels shall include a Gray Network Firewall.	F	T
VPN-FW-11	All physical paths within the Gray network between two Inner VPN Components for Red networks of different security levels shall include a Gray Network Firewall.	F	O
VPN-FW-12	All physical paths within the Gray network between a Gray CA or an Administration Workstation and an Inner VPN Component for a Red network whose classification level is lower than the highest classification of data protected by the solution shall include a Gray Network Firewall.	F	T=O

10.12 Requirements for CDP Devices

Table 18. Requirements for CDP Devices

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-CD-1	The CRL hosted by the Outer CDP shall not contain extensions other than what is specified in RFC 5280.	C	T=O
VPN-CD-2	The CRL hosted on the Inner CDP shall be signed by the Red Network CA.	C	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-CD-3	The CRL hosted on the Outer CDP shall be signed by the Gray Network CA.	C	T=O
VPN-CD-4	CRL Distribution Points (CDPs) shall only issue CRLs over port 80 (HTTP).	C	T=O
VPN-CD-5	CRLs shall be transferred via an AO-approved one-way transfer mechanism from the Red Network CA to the Inner CDP server.	C	T=O
VPN-CD-6	CRLs shall be transferred via an AO-approved one-way transfer mechanism from the Gray Network CA to the Outer CDP server.	C	T=O
VPN-CD-7	CRLs shall be transferred to a CDP server at least 4 days prior to the expiration of the current CRL.	C	T=O
VPN-CD-8	VPN Gateways shall check the age of the cached CRL prior to the establishment of new connections. If the age of the cached CRL is greater than an hour, then it shall download an updated CRL from the CDP prior to authenticating the new connection.	C	T=O
VPN-CD-9	Gateways shall load the CRL from the CDP at least 3 days prior to the expiration of the current CRL.	C	T=O
VPN-CD-10	All CDPs shall only allow outbound traffic on ports 80 and ports used for remote management traffic that adheres to VPN-RA-1.	C	T=O
VPN-CD-11	Traffic filtering rules on the CDPs shall be applied based on known VPN Component addresses or address ranges to further protect against unknown IPsec traffic.	C	T=O
VPN-CD-12	The Red Network CA shall issue the CRL for the Inner CDP.	C	T=O
VPN-CD-13	The Gray Network CA shall issue the CRL for the Outer CDP.	C	T=O
VPN-CD-14	If integrity check of the CRL pulled from the CDP fails, then the VPN Component shall use the current cached CRL.	C	T=O
VPN-CD-15	If the CDP is down or contains an invalid CRL, then the Inner and Outer VPN Gateway's CRLs shall be manually updated prior to the expiration of the current CRLs.	C	T=O
VPN-CD-16	The Red Network CA shall set the CRL Distribution Points extension of the certificates it generates for the VPN solution to the list of URLs hosted by Inner CDPs from which Inner VPN Components can download the CRL.	C	T=O
VPN-CD-17	The Gray Network CA shall set the CRL Distribution Points extension of the certificates it generates for the VPN solution to the list of URLs hosted by Outer CDPs from which Outer VPN Components can download the CRL.	C	T=O

11 GUIDANCE FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

Table 19. Guidance for the Use and Handling of Solutions

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-GD-1	All components of the solution, with the exception of Remote EUDs when powered off, shall be physically protected as classified devices, classified at the level of the network with the highest classification in the solution or in any other VPN solutions it interconnects with..	M, R, L	T=O
VPN-GD-2	Remote EUDs shall be handled as unclassified devices when powered off in accordance with AO procedures.	R	T=O
VPN-GD-3	Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the infrastructure components.	M, R, L	T=O
VPN-GD-4	Only authorized and appropriately cleared users, administrators, and security personnel shall have physical access to EUDs.	R, L	T=O
VPN-GD-5	All components of the solution, with the exception of Remote EUDs, shall be disposed of as classified devices, unless declassified using AO/DAA-approved procedures.	M, R, L	T=O
VPN-GD-6	Remote EUDs with NSA-approved DAR solution shall be disposed of in accordance with disposal requirements for the DAR solution.	R	T=O
VPN-GD-7	Remote EUDs that do not store classified data, and consequently do not include an NSA-approved DAR solution, shall be disposed of as unclassified devices in accordance with AO/DAA-approved procedures.	R	T=O
VPN-GD-8	All EUDs shall have their certificates revoked prior to disposal.	R, L	T=O
VPN-GD-9	Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.	M, R, L	T=O
VPN-GD-10	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the Capability Package.	M, R, L	T=O
VPN-GD-11	The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the VPN Capability Package.	M, R, L	T=O
VPN-GD-12	Results of the compliance audit shall be provided to and reviewed by the AO/DAA.	M, R, L	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-GD-13	When a new approved version of the VPN Capability Package is published by NSA, the AO/DAA shall ensure compliance against this new Capability Package within 6 months.	M, R, L	T=O
VPN-GD-14	Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or less) months (see Section 13.3).	M, R, L	T=O
VPN-GD-15	Audit log data shall be maintained for a minimum of 1 year.	M, R, L	T=O
VPN-GD-16	The amount of storage remaining for audit events shall be assessed quarterly in order to ensure that adequate memory space is available to continue recording new audit events.	M, R, L	T=O
VPN-GD-17	Audit data shall be frequently offloaded to a backup storage medium.	M, R, L	T=O
VPN-GD-18	A set of procedures shall be developed by the implementing organization to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	M, R, L	T=O
VPN-GD-19	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	M, R, L	T=O
VPN-GD-20	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long-term storage.	M, R, L	T=O
VPN-GD-21	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product.	M, R, L	T=O
VPN-GD-22	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	M, R, L	T=O
VPN-GD-23	Strong passwords shall be used that comply with the requirements of the local security authority.	M, R, L	T=O
VPN-GD-24	Security critical patches (such as IAVAs) shall be tested and subsequently applied to all components in the solution in accordance with local policy and this Capability Package.	M, R, L	T=O
VPN-GD-25	Local policy shall dictate how the Security Administrator will install patches to solution components.	M, R, L	T=O
VPN-GD-26	Solution components shall comply with local TEMPEST policy.	M, R, L	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-GD-27	Software, settings, keys, and all other configuration data persistently stored on Remote EUD shall be handled as controlled unclassified information.	R	T=O

Additional policy can be found in Section 12.

12 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the VPN solution within a single site. Security Administrator duties include but are not limited to:

1) Ensuring that the latest security critical software patches and updates (such as IAVAs) are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the VPN solution.

5) Ensuring that the implemented VPN solution remains compliant with the latest version of this Capability Package.

6) Provisioning and maintaining EUDs in accordance with this Capability Package for implementations which include them.

Certificate Authority Administrator (CAA) – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to:

1) Administering the CA, including authentication of all components requesting certificates.

2) Maintaining and updating the Certificate Revocation List (CRL).

3) Provisioning and maintaining EUD certificates in accordance with this Capability Package for implementations which include them.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the wired VPN solution. The role of Auditor and Security Administrator shall not be performed by the same individual. Auditor duties include but are not limited to:

1) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting security related incidents to the appropriate authorities.

3) The Auditor will only be authorized access to the Outer and Inner admin components.

Solution Integrator – In certain cases, an external integrator may be hired to implement a VPN solution based on this Capability Package. Solution Integrator duties may include but are not limited to:

1) Acquiring the products that compose the solution.

2) Configuring the VPN solution in accordance with this Capability Package.

Remote User –A Remote User may operate a Remote EUD from physical locations not owned, operated, or controlled by the government. The Remote User shall be responsible for operating the Remote EUD in accordance with this Capability Package and an organization defined user agreement. Remote User duties include, but are not limited to:

1) Ensuring the Remote EUD is only operated in physical spaces which comply with the end user agreement.

2) Alerting the Security Administrator immediately upon a Remote EUD being lost, stolen, or suspected of being tampered with.

Additional policies related to the personnel that perform these roles in a VPN Solution are as follows:

Table 20. Role-Based Personnel Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-GD-28	The Security Administrator, CAAs, Auditor, Remote User, and all Solution Integrators shall be cleared to the highest level of data protected by the VPN solution. When an Enterprise CA is used in the solution, the CAA already in place may also support this solution, provided they meet this requirement.	M, R, L	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-GD-29	The Security Administrator, CAA, and Auditor roles shall be performed by different people.	M, R, L	T=O
VPN-GD-30	All Security Administrators, CAAs, Remote Users, and Auditors shall meet local information assurance training requirements.	M, R, L	T=O
VPN-GD-31	The CAA(s) for the Inner tunnel shall be different from the CAA(s) for the Outer tunnel.	M, R, L	T=O
VPN-GD-32	Upon discovering an EUD is lost or stolen, a Remote User shall immediately report the incident to their System Administrator and Certificate Authority Administrator.	R	T=O
VPN-GD-33	Upon notification of a lost or stolen EUD, the Certificate Authority Administrators shall revoke the EUD certificates.	R	T=O
VPN-GD-34	*Superseded by VPN-KM-26*		
VPN-GD-35	Remote Users shall not store classified information on any Remote EUD that does not implement an NSA-approved data-at-rest (DAR) solution.	R	T=O

13 INFORMATION TO SUPPORT AO/DAA

This section details items that likely will be necessary for the customer to obtain approval from the system AO/DAA. The customer and AO/DAA have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved Capability Package.
- The customer has a testing team develop a Test Plan and perform testing of the VPN solution, see Section 13.1.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 13.2.
- The customer provides the results from testing and system certification and accreditation to the AO/DAA for use in making an approval decision. The AO/DAA is ultimately responsible for ensuring that all requirements from the Capability Package have been properly implemented.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 13.3.
- Customers who want to use a variant of the solution detailed in this Capability Package will contact NSA to determine ways to obtain NSA approval.

- The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the VPN Capability Package, and the results shall be provided to the AO/DAA.
- The AO/DAA will ensure that certificate revocation information is updated on all the VPN Gateways in the solution in the case of a compromise.
- The AO/DAA will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.

The system AO/DAA maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO/DAA shall ensure that the solution remains properly configured, with all required security updates implemented.

13.1 Solution Testing

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a VPN solution. This T&E will be a critical part of the approval process for the AO/DAA, providing a robust body of evidence that shows compliance with this Capability Package.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the VPN solution. The entire solution, to include each component described in Section 5, is addressed by this test plan.

1) Set up the baseline network architecture and configure all components.
2) Document the baseline network architecture configuration. Include product model and serial numbers, and software version numbers as a minimum.
3) Develop a Test Plan for the specific implementation using the test objectives from Section 14. Any additional requirements imposed by the local AO/DAA should also be tested, and the Test Plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this Capability Package.
4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO/DAA for approval of the solution.

The following testing requirement has been developed to ensure that the VPN solution functions properly and meets the configuration requirements from Section 10. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 21. Test Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
VPN-TR-1	The organization implementing the Capability Package shall perform all tests listed in Section 14.	M, R, L	T=O

13.2 Risk Assessment

The risk assessment of the VPN solution presented in this Capability Package focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the SIPRNet CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO/DAA shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

13.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. This registration will allow NSA to track where VPN Capability Package solutions are instantiated and to provide AO/DAAs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components/architectures approved for these solutions. The CSfC solution registration process is available at http://www.nsa.gov/ia/programs/csfc_program.

Solutions designed to this Capability Package may be used for one year, and must then be revalidated against the current Capability Package. Approved Capability Packages will be reviewed twice a year, or as events warrant. Notification of these updates will be provided to all registered users of the Capability Package.

14 TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure they have properly configured the solution. As defined in Section 8, in order to comply with this Capability Package, a solution must at minimum implement all Threshold requirements associated with each of the architectures it supports, and should implement the Objective requirements associated with those architectures where feasible. These tests may also be used to provide evidence to the AO/DAA regarding compliance of the solution with this Capability Package. Note that the details of the

procedures are the responsibility of the final developer of the test plan in accordance with AO/DAA-approved network procedures. The AO/DAA is ultimately responsible for ensuring that all requirements from the Capability Package have been properly implemented.

14.1 Product Selection

This section contains a procedure to verify that the components in this CP were selected to ensure independence in several important features.

Requirements being tested: VPN-PS-1 through VPN-PS-12, VPN-SR-3, VPN-SR-6

Procedure Description:

1) For each VPN Component, perform the following:
    a) Inspect the Inner and Outer VPN Gateways are on the list of IPsec VPN Gateways on the CSfC Components List. (VPN-PS-1)
    b) Inspect the Inner and Outer VPN Client came from the list of IPsec VPN Clients on the CSfC Components List. (VPN-PS-2)
    c) Inspect the Inner and Outer VPN Gateways come from different vendors and the vendors are not subsidiary of each other. (VPN-PS-4)
    d) Inspect the Inner and Outer VPN Gateways are logically separated using an NSA-approved mechanism. (VPN-PS-5)
    e) Inspect the Inner and Outer VPN Gateways are running on physically separate hardware platforms. (VPN-PS-6)
    f) Inspect the Inner and Outer VPN Gateways are running differing Operating Systems for critical IA security functionality. (VPN-PS-7)
    g) Inspect the implementation of the Inner and Outer VPN Gateway cryptographic libraries come from different vendors. (VPN-PS-10)
2) For each Certificate Authority (CA), perform the following:
    a) Inspect the Inner and Outer tunnel CAs came from the list of CAs on the CSfC Components List or are Enterprise CAs. (VPN-PS-3)
    b) Inspect that the Inner and Outer tunnel CAs came from different vendors. (VPN-PS-8)
    c) Verify that the Inner and Outer CA cryptographic libraries come from different vendors. (VPN-PS-12)

3) For each VPN client, perform the following:

   a) Inspect the Inner and Outer VPN clients vendors came from different vendors. (VPN-PS-9)

   b) Inspect the implementation of the Inner and Outer VPN clients' software cryptographic libraries are from different vendors. (VPN-PS-11)

4) For all components used, review the mitigations in the Product Supply Chain Threat Assessment. Ensure that mitigations identified in the assessment are implemented according to the implementing organization's AO/DAA approved Product Supply Chain Threat Assessment process. (VPN-PS-13)

5) For sites requiring interoperability, ensure that VPN Gateways selected for each tunnel can be configured to communicate using the requirements specified in this Capability Package. (VPN-SR-3)

6) For sites using an EUD, ensure that the VPN client on the EUD is configured to communicate with the corresponding VPN Gateway. (VPN-SR-6)

Expected Result:

The results of the inspection should reveal that the VPN Solution components conform to the VPN CP; results are pass/fail.

14.2 Physical Layout of Solution

This section contains a procedure to create an accurate record of the physical components composing the VPN solution (including workstations, VPN Gateways, CA, and wiring). The test will also ensure that the physical implementation of the VPN solution matches one of the architectures given in the VPN Capability Package.

Requirements being tested: VPN-SR-1, VPN-SR-2, VPN-CR-10

Procedure Description:

1) Ensure there are no wireless or physical connection to the solution that are not included in this Capability Package, which may allow for traffic to leave the Red or Gray network in a manner that does not go through the VPN solution (or an NSA-certified encryptor). (VPN-CR-10)

2) Ensure the Gray Management network is cryptographically separate and connected through a dedicated management port on the Outer VPN Gateway that is separate from the port used for the Gray data network. (VPN-SR-1)

3) Verify the physical location of any network architecture component for the Outer VPN Gateway is located on the Gray Management network. Similarly, these components for the Inner VPN Gateway will be located on the Red network. (VPN-SR-2)

Expected Result:

For Step 1, there should be no extraneous wireless or physical connections allowing data to leave the Red or Gray networks besides through the VPN solution (or an NSA-certified encryptor). For Step 2, the Gray Management network traffic should be separate from the Gray network traffic. For Step 3, network architecture components should be located inside the network.

14.3 End User Device Configurations

This section contains a procedure to ensure that the configurations for all the EUDs in the VPN solution follow the requirements given in this Capability Package.

Requirements being tested: VPN-EU-1 through VPN-EU-18

Procedure Description:

1) For each EUD perform the following:

   a) Verify that the Security Administrator is the only role that can use external data storage media on the EUD. (VPN-EU-3)

   b) Inspect the implementing organization policy states that provisioning the EUD takes places in a facility that is equal to highest classification level of the VPN solution. (VPN-EU-6)

   c) Inspect the EUD's BIOS in order to verify that the BIOS comply with the security guidelines found in NIST SP 800-147. (VPN-EU-13)

   d) Log into the EUD as a normal user. Then log into the central server to ensure that this activity is captured in the log. (VPN-EU-17)

   e) Ensure that the implementing organization's policy states that the EUD is dedicated for use within the VPN Solution. (VPN-EU-18)

2) For each Remote EUD perform the following:

   a) Inspect that the EUD prohibits the local storage of user data from the Red network and the use of external data storage media or it is using an NSA-Approved DAR solution. (VPN-EU-1)

   b) Inspect the Full Disk Encryption for the EUD is FIPS 140-2 (or later) validated or NSA-approved DAR solution. (VPN-EU-2)

c) Verify that Red network services do not transmit any classified data to the EUD until user authentication succeeds. (VPN-EU-11, VPN-EU-12)

3) For each EUD that directly connects to a Black network, perform the following:

a) Inspect the Inner and Outer VPN Clients on the EUD and verify that separate private key stores are used. (VPN-EU-4)

b) Verify that the Inner and Outer VPN Clients on the EUD are implemented on separate IP stacks. (VPN-EU-5)

4) If the EUD is not remotely administrated, verify that procedure given in VPN-EU-7 is followed and/or is currently in place.

5) Verify that the procedures given in VPN-EU-8, VPN-EU-9, and VPN-EU-10 are followed and/or currently in place.

6) Inspect the implementing organization's policy that all Remote Access users must sign an organization defined user agreement prior to using the EUD. (VPN-EU-14)

7) Verify that the implementing organization has a training program in place for Remote Access users operating an EUD. (VPN-EU-15)

8) Verify that the implementing organization has a user agreement for EUD users and also polices for each element within their user agreement document. (VPN-EU-16)

Expected Result:

For step 1-3, all EUDs shall be configured properly. For step 4-5, a remotely administrated EUD shall only be rekeyed over the VPN solution network prior to the expiration of keys. If this cannot be accomplished, the EUD must be re-provisioned. For steps 6-8, the implementing organization should have policies in place in order to address the requirements identified.

14.4 VPN Component Configurations

This section contains a procedure to ensure that the configurations for all the VPN Components in the VPN solution follow the requirements given in this Capability Package.

Requirements being tested: VPN-SR-4, VPN-SR-5, VPN-SR-7, VPN-SR-8, VPN-CR-1 through VPN-CR-8, VPN-CR-11 through VPN-CR-22, VPN-IR-1 through VPN-IR-4, VPN-OR-1 through VPN-OR-6, VPN-RA-1 through VPN-RA-9, VPN-KM-7, VPN-KM-8, VPN-PF-1 through VPN-PF-7

Procedure Description:

1) For each VPN component in the solution, perform the following:

   a) Obtain the current configuration for the VPN Component.

   b) Verify a unique device certificate is loaded with the corresponding CA signing certificate. (VPN-CR-5)

   c) Verify a device certificate from a CA included in the VPN solution is listed in the configuration for authentication. (VPN-CR-6)

   d) Ensure the corresponding CA signing certificate and certificate revocation information are on the VPN Component. (VPN-CR-7)

   e) Verify the requirements VPN-CR-1 through VPN-CR-4, VPN-CR-8, VPN-CR-11 through VPN-CR-22, and VPN-PF-1 through VPN-PF-3, VPN-SR-7 through VPN-SR-8 are configured properly.

   f) Ensure the time of day matches the current time. This should be within a small margin of error, to be determined by the AO/DAA. (VPN-SR-4, VPN-SR-5)

2) For each Inner VPN component in the solution, use the configuration from 1a and perform the following:

   a) Log into the Inner VPN components and verify that they are configured to use Tunnel or Transport mode IPsec with an associated IP Protocol (e.g., GRE). (VPN-IR-1)

   b) Log into the Inner VPN components and verify that the MTU (for IPv4) or the PMTU (for IPv6) has been configured to an appropriate size. (VPN-IR-2)

   c) Using a packet analyzer tool on the Inner VPN Gateway, verify that traffic leaving the external interface going to the Outer VPN Gateway is encrypted. (VPN-IR-3)

   d) Using a packet analyzer tool on the EUD, ensure that all traffic leaving the Inner VPN client is encrypted except for traffic identify in this CP. (VPN-IR-4)

   e) Verify all CA signing certificates used for these components are from Inner tunnel CAs. (VPN-KM-7)

3) For each Outer VPN component in the solution, use the configuration from 1a and perform the following:

   a) Log into the Outer VPN components and verify that they are configured to use Tunnel mode IPsec. (VPN-OR-1)

   b) Verify that VPN-OR-2, VPN-OR-3, and VPN-PF-6 through VPN-PF-7 have been configured.

c) Using a packet analyzer tool on the EUD, ensure that all traffic leaving the Outer VPN client is encrypted except for traffic identify in this CP. (VPN-OR-4)

d) Using a packet analyzer tool on the EUD, verify that traffic leaving the EUD is encrypted by the Inner VPN client. (VPN-OR-5)

e) Verify that all CA signing certificates used for these components are from Outer tunnel CAs. (VPN-KM-8)

4) Inspect the configuration files state that the Outer VPN component or the EUD communications to a third party server are blocked. (VPN-PF-6)

5) Inspect the configuration files state that the Outer VPN component and the EUD communications to a third party server are disabled. (VPN-PF-7)

6) For an EUD that uses virtual machines to separate the Inner and Outer VPN clients, verify that the Outer VPN Client are not installed on the host operating system. (VPN-OR-6)

7) For an EUD, inspect the configuration file allows remote management and that local management is disabled. (VPN-RA-2)

8) For each VPN Gateway, attempt that the private key cannot be accessed through any interface. (VPN-CR-9)

9) For all device administration, verify that requirements VPN-RA-1 and VPN-RA-3 through 7 are configured properly.

10) For each administration workstation, ensure the Security Administrator is required to authenticate to the component before being granted access. (VPN-RA-8)

11) For each administration workstation, ensure the Security Administrator is required to authentication to solution components using Suite B compliant certificates through. (VPN-RA-9)

Expected Result:

For Steps 1-8, all VPN Components should be configured properly according to the requirements found in this Capability Package. For Steps 9-11, all VPN Component administration devices should be configured properly based upon the requirements of this Capability Package.

14.5 CA CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all of the CAs used within the VPN solution follow the requirements given in this Capability Package.

Requirements being tested: VPN-KM-1 through VPN-KM-6, VPN-KM-10 through VPN-KM-24

Procedure Description:

1) Verify requirements VPN-KM-1 through VPN-KM-6, and VPN-KM-10 are met by both CAs.
2) Verify if the Inner tunnel CA and Outer tunnel CA are an Enterprise CA that it meets requirements VPN-KM-17 and VPN-KM-18.
3) Verify requirements VPN-KM-19 through VPN-KM-24 are met by any Locally-run CA.
4) Verify the VPN Gateways were keyed in a manner consistent with VPN-KM-11 through VPN-KM-14.
5) Ensure there is certificate revocation information and CA signing certificate on each VPN Components. (VPN-KM-15)
6) Review the implementing organization's policy for how new certificates are to be issued. As a Certificate Authority Administrator issue a certificate for a new user in accordance with the policy. (VPN-KM-16)

Expected Result:

For Steps 1-6, all CAs should be configured to meet the requirements being tested from Section 10.10 of this Capability Package.

14.6 CRL Requirements for CAs

This section contains procedures for ensuring that policy is in place for CRLs of CAs.

Requirements being tested: VPN-KM-25 through VPN-KM-28

Procedure Description:

1) Verify that the implementing organization has an approved policy in place that states that the CA shall generate an updated CRL within 1 hour of a certificate revocation. (VPN-KM-25)
2) Verify that the implementing organization has an approved policy in place that states that when a certificate is revoked, the updated CRL shall be distributed to the VPN gateways within 24 hours of revocation. (VPN-KM-26)
3) Verify that the implementing organization has an approved policy in place that states that CRLs shall expire no later than 31 days after their issue date. (VPN-KM-27)
4) Verify that the information contained within the CRL complies with RFC5280. (VPN-KM-28)

a) Pull down a valid CRL from the Red Network CA and Gray Network CA

b) Verify that the information contained within the CRL complies with RFC5280.

Expected Result:

For steps 1-3, the implementing organization should have policies in place to address the requirements identified. For step 4, CRL information will comply with RFC5280.

14.7 EUD With Multiple Connections

This section contains a procedure to ensure that only one connection is allowed per EUD and that the second connection is immediately dropped.

Requirements being tested: VPN-AU-21 through VPN-AU-23

Procedure Description:

5) The administrator will install the same device certificates on two EUDs.

6) The administrator will authenticate to the Red network. At the same time, the Auditor will be reviewing the logs and detect that the same device certificate is coming from two different devices. (VPN-AU-21)

7) The Auditor will alert the Certificate Authority Administrator to revoke the certificates and provide an updated Certification Revocation List to the Security Administrator. (VPN-AU-22)

8) Once the Security Administrator receives notification from the Certificate Authority Administrator, the Security Administrator will drop both sessions. (VPN-AU-23)

Expected Result:

The same device certificate cannot be used for two devices. All results are expected to be pass/fail.

14.8 Use of Certificates from Trusted CAs

This section contains a procedure to ensure that public/private key and certificates are only used for authentication only from trusted CAs are accepted.

Requirements being tested: VPN-KM-9, VPN-AU-8, VPN-AU-25

Procedure Description:

1) Ensure that the solution is in its default setting and that the VPN connections are established when the proper certificates (see Section 6) are used to authenticate the VPN Gateways.

2) Install approved certificates on the VPN Gateways, generated by the approved CAs, and configure the solution so that one of the VPN Gateways uses this certificate for authentication. (VPN-KM-9)

   a) Verify an entry to the Audit log has been created due to certificate loading. (VPN-AU-8)

   b) Start the VPN connections using the new configuration.

   c) Verify the connection is successful; end-to-end communication is provided because the Gateways will authenticate. Verify that success is logged in the audit data.

   d) Repeat this test for each VPN Gateway.

3) When testing is complete, remove the alternate certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion and the log is sent to the centralized host. (VPN-AU-8, VPN-AU-25)

Expected Result:

Authentication will occur when the VPN Gateways identify the trust anchor of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

14.9 Use of Revoked Certificates

This section contains a procedure to ensure that only valid certificates are accepted. This section focuses on certificates that have been revoked (and are therefore invalid) and does not include all types of validity testing.

Requirements being tested: VPN-KM-7 through VPN-KM-8, VPN-KM-15, VPN-AU-8, VPN-AU-10

Procedure Description:

1) Ensure the solution is in its default setting and that the VPN connections are established when the proper, valid certificates (see Section 6) are used to authenticate the VPN Gateways.

2) Revoke a certificate for one of the VPN Gateways (or install an alternate revoked certificate on one of the VPN Gateways), and ensure the solution is configured so that this revoked certificate will be used for authentication.

   a) If applicable, verify that an entry to the Audit log has been created due to certificate loading. (VPN-AU-8)

   b) Ensure the VPN Gateways contain the latest certificate revocation information to include the revoked certificate to be used for authentication. (VPN-KM-15)

   c) Start the VPN connection.

d) Verify that the connection is not successful; end-to-end communication is not provided because the Gateways will fail to authenticate the revoked certificate. Verify that failures are logged in the audit data. (VPN-KM-7, VPN-KM-8, VPN-AU-10)

e) Repeat this test for each VPN Gateway; only one VPN Gateway should offer the revoked certificate per connection.

3) When testing is complete, remove the revoked certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion. (VPN-AU-8)

Expected Result:

Authentication will not occur when the VPN Gateways cannot verify the validity of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

14.10 Configuration Change Detection

This section contains a procedure to ensure that changes made to any of the VPN Component configurations are detected by the Configuration Change Detection tool.

Requirements being tested: VPN-CM-1 through VPN-CM-3

Procedure Description:

1) The following steps shall be performed for each of the VPN Component within the solution.

a) Log into the VPN Component.

b) Compare the current version of the VPN Component configuration with the stored baseline and ensure the current version matches the stored configuration. (VPN-CM-1)

c) Make a change to the configuration, preferably something that is not fundamental to the security of the VPN solution.

d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from c) are recorded. (VPN-CM-2, VPN-CM-3)

Expected Result:

The Auditor will validate the baseline configuration was stored in Step 1b. In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change.

14.11 AUDIT

This section contains procedures for ensuring audit events are detected, the proper information is logged for each event, and there is a procedure detailed in the CPS documentation for auditing each CA device.

Requirements being tested: VPN-AU-1 through VPN-AU-7, VPN-AU-9, VPN-AU-11 through VPN-AU-20, VPN-AU-24

Procedure Description:

1) Examples for testing the ability of each VPN Component to audit and log audit events specified in the CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry in accordance with Section 10.9.

    a) All actions performed by a user with super privileges (auditor, administrator, etc.) and any escalation of user privileges. (VPN-AU-6, VPN-AU-7)

        i) Log in as an administrator to the VPN Gateway.

        ii) Perform a variety of administrator actions on the VPN Gateway.

        iii) Verify a log entry was created for each action taken in Step ii that required super-user privileges and also states the escalation or privileges.

        iv) Revert back to the baseline configuration, eliminating the changes made in Step ii.

        v) Repeat the above with the Auditor role.

    b) Changes to time. (VPN-AU-9, VPN-AU-20)

        i) Log in as a Security Administrator to the VPN Gateway.

        ii) Modify the system time on the VPN Gateway by at least 1 hour.

        iii) Verify a log entry was created due to the change in system time and by whom.

        iv) Revert the system time back to the accurate time of day.

    c) Log into and out of the VPN Solution as a normal user and send traffic to the Red Network. Then log into the central log server as an Auditor, and inspect the audit entry for the following: (VPN-AU-24)

        i) Verify that the log on as a normal user is logged and has an identifiable code for the type of event. (VPN-AU-4, VPN-AU16)

ii) Identifies the subject accessing the solution. (VPN-AU-18)

iii) Identify the identifier of the event. (VPN-AU-15)

iv) States the time, date, and the time zone offset. (VPN-AU-14)

d) Establish and terminate a VPN tunnel. Verify in the logs, that these two events were logged. (VPN-AU-1, VPN-AU-2)

e) All built-in self-test results, which may indicate failures in cryptographic functionality. (VPN-AU-12)

i) Completely power down the VPN Gateway.

ii) Power the VPN Gateway back up so that the automatic self-tests are run.

iii) Verify a log entry was created due to running the self-tests.

f) Log into a VPN Gateway as a Security Administrator and delete the previous week's audit log. Verify the log recorded this deletion. (VPN-AU-3)

g) As the Certificate Administrator, log into the audit log and attempt to delete a log entry. Verify this action is recorded with a failure code. (VPN-AU-5, VPN-AU-17)

2) Verify the source address for all audit log entries is recorded. (VPN-AU-19)

3) Verify there is a procedure detailed in the CPS documentation for auditing each CA device within the solution. (VPN-AU-13)

4) Inspect the organization's implementing policy states audit logs are monitored by the Auditor at least weekly. (VPN-AU-11)

Expected Result:

For step 1, all occurrences of auditable events given in should generate an entry in the audit log. For step 2, the source address should be the VPN Gateway's loopback address. For step 3, there should be a procedure for auditing the CA devices in the solution outlined in the CPS document. For step 4, ensure the implementing organization has a policy that complies with this requirement.

14.12 Implementation of Guidance

This section ensures there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the VPN solution. It also ensures the personnel are in place to manage and administer this solution follow the guidelines given in the Capability Package.

Requirements being tested: VPN-GD-1 through VPN-GD-35

Procedure Description:

1) Verify the procedures given in VPN-GD-1 through VPN-GD-9, VPN-GD-15 through VPN-GD-27, and VPN-GD-32 through VPN-GD-35 were/are followed and/or are currently in place.
2) Verify the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (VPN-GD-10)
3) Verify the solution owner and AO/DAA are aware that a compliance audit will be conducted every year. (VPN-GD-11)
4) Verify the AO/DAA is aware that they shall receive the results of the compliance audit and are responsible for reviewing. (VPN-GD-12)
5) Verify the solution owner and AO/DAA are aware that when new versions of the VPN Capability Package are published by NSA, they will have 6 months to move into compliance with this new version. (VPN-GD-13)
6) Verify the solution owner and AO/DAA are aware that they shall provide updated solution information to NSA on a yearly basis. (VPN-GD-14)
7) Verify the personnel requirements given in VPN-GD-28 through VPN-GD-31 are met by the personnel supporting this implementation of the VPN solution.

Expected Result:

For 1-7, all of these procedures have been followed or are in place.

14.13 Solution Functionality

This section contains a procedure for ensuring the implementing organization complies with the testing requirements.

Requirements being tested: VPN-TR-1

Procedure Description:

1) The implementing organization's DAA will inspect the test report in order to ensure all testing requirements have been met. (VPN-TR-1)

Expected Result:

The report will ensure the implementing organization complies with the VPN Solution.

14.14 Gray Network Firewall Placement

This section contains a procedure for ensuring that the placement of Gray Network Firewalls within the solution complies with the requirements of this Capability Package.

Requirements being tested: VPN-FW-7, VPN-FW-10, VPN-FW-11, VPN-FW-12

Procedure Description:

1) For each Gray Network Firewall within the solution:
   a) Verify that it does not also function as an Inner VPN Gateway. (VPN-FW-7)
2) For each Inner VPN Gateway within the solution:
   a) Verify that every physical path through the Gray network between it and another Inner VPN Gateway for a Red network of a different classification level contains at least one Gray Network Firewall. This includes Inner VPN Gateways located at other sites that the solution connects with. (VPN-FW-10)
   b) Verify that every physical path through the Gray network between it and another Inner VPN Gateway for a Red network of a different security level contains at least one Gray Network Firewall. This includes Inner VPN Gateways located at other sites that the solution connects with. (VPN-FW-11)
   c) If the Inner VPN Gateway protects a Red network of a classification level lower than the highest classification level protected by the overall system, verify that every physical path through the Gray network and a Certificate Authority, Administration Workstation, or CDP contains at least one Gray Network Firewall. This includes Certificate Authorities, Administration Workstations, and CDPs located at other sites that the solution connects with. (VPN-FW-12)

Expected Result:

In Step 1, the Inner VPN Gateways and Gray Network Firewalls are verified to be separate physical devices. In Step 2, Gray Network Firewalls are verified to be placed at all appropriate positions within the Gray network.

14.15 Gray Network Firewall IPsec Filtering Rules

This section contains a procedure for ensuring that the filtering rules on Gray Network Firewalls are configured so that the only IPsec traffic allowed through the firewall is between Inner VPN Gateways that are allowed to establish VPN tunnels with one another.

Requirements being tested: VPN-AU-29, VPN-FW-1, VPN-FW-6, VPN-FW-9

Procedure Description:

1) For each Inner VPN Gateway within the solution (hereafter referred to as Inner VPN Gateway A):

   a) For each other Inner VPN Gateway within the solution that protects a Red network of the same security level:

      i) Attempt to establish an IPsec VPN connection to it from Inner VPN Gateway A..

      ii) Verify that the VPN connection was established. (VPN-FW-1, VPN-FW-6)

   b) For each Inner VPN Gateway within the solution that protects a Red network of a different security level (hereafter referred to as Inner VPN Gateway B):

      i) Identify the first Gray Network Firewall on the physical path from Inner VPN Gateway A and Inner VPN Gateway B.

      ii) Place a packet sniffer on the interface of the Gray Network Firewall facing Inner VPN Gateway B.

      iii) Attempt to establish an IPsec VPN connection from Inner VPN Gateway A to Inner VPN Gateway B.

      iv) Verify that the VPN connection was not established.

      v) Verify that the packet sniffer did not record any IKE or IPsec packets with a source address of Inner VPN Gateway A and a destination address of Inner VPN Gateway B. (VPN-FW-9)

      vi) Verify that the Gray Network Firewall logs contain an event for an IKE or IPsec packet with a source address of Inner VPN Gateway A and a destination address of Inner VPN Gateway B. (VPN-AU-29)

Expected Result:

In Step 1(a), the Gray Network Firewall allows IKE and IPsec traffic between pairs of Inner VPN Gateways that are allowed to establish VPN tunnels with one another. In Step 1(b), the Gray Network Firewall denies IKE and IPsec traffic between pairs of Inner VPN Gateways that protect Red networks of different classification levels.

14.16 Gray Network Firewall HTTP Filtering Rules

This section contains a procedure for ensuring that the filtering rules on Gray Network Firewalls are configured so that the only HTTP traffic allowed through the firewall is from an Inner VPN Component to an Inner CDP.

Requirements being tested: VPN-AU-29, VPN-FW-2, VPN-FW-9

Procedure Description:

1) For each Inner VPN Component within the solution:

   a) For each Inner CDP within the solution:

      i) Attempt to have the Inner VPN Component download the current CRL from the Inner CDP.

      ii) Verify that the download was successful. (VPN-FW-2)

      iii) Identify the first Gray Network Firewall on the physical path from the Inner VPN Component to the Inner CDP. If no such Gray Network Firewall exists, skip the remainder of Step 1(a).

      iv) Place a packet sniffer on the interface of the Gray Network Firewall facing the Inner VPN Component.

      v) From the Inner CDP, attempt to make an HTTP request to the Inner VPN Component.

      vi) Verify that the request failed.

      vii) Verify that the packet sniffer did not record any packets with a source address of the Inner CDP and a destination address of the Inner VPN Component. (VPN-FW-9)

      viii) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the Inner CDP and a destination address of the Inner VPN Component. (VPN-AU-29)

   b) For every other device on the Gray network that is not an Inner CDP:

      i) Identify the first Gray Network Firewall on the physical path from the Inner VPN Component to the other device. If no such Gray Network Firewall exists, skip the remainder of Step 1(b).

      ii) Place a packet sniffer to the interface of the Gray Network Firewall facing the other device.

      iii) Attempt to have the Inner VPN Component download a CRL from the other device.

      iv) Verify that the download failed.

      v) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Component and a destination address of the other device. (VPN-FW-9)

      vi) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the Inner VPN Component and a destination address of the other device. (VPN-AU-29)

Expected Results:

In Step 1(a), the Gray Network Firewall allows HTTP requests from the Inner VPN Component to the Inner CDP, but not from the Inner CDP to the Inner VPN Component. In Step 1(b), the Gray Network Firewall denies HTTP requests from the Inner VPN Component to devices that are not Inner CDPs.

14.17 Gray Network Firewall Management

This section contains a procedure for ensuring that Gray Network Firewalls can only be managed from the Administration Workstation on the Gray Management network.

Requirements being tested: VPN-AU-29, VPN-FW-5

Procedure Description:

1) For each Gray Network Firewall within the solution:
    a) From the Administration Workstation on the Gray Management network, attempt to connect to the Gray Network Firewall's remote management interface.
    b) Verify that the connection attempt was successful. (VPN-FW-5)
    c) For each physical network interface on the Gray Network Firewall except the one through which the Administration Workstation connects:
        i) From a device reachable from the physical network interface, attempt to connect to the Gray Network Firewall's remote management interface.
        ii) Verify that the connection attempt failed. (VPN-FW-5)
        iii) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the selected device and a destination address of the Gray Network Firewall. (VPN-AU-29)

Expected Results:

In Step 1(b), the Gray Network Firewall allows management traffic from the Administration Workstation. In Step 1(c), the Gray Network Firewall blocks attempts to access the management interface through other physical network interfaces.

14.18 Gray Network Firewall Address Spoofing

This section contains a procedure for ensuring that Gray Network Firewalls detect spoofing of source addresses in traffic sent through it.

Requirements being tested: VPN-AU-29, VPN-FW-8

Procedure Description:

1) For each Gray Network Firewall within the solution:

   a) For each physical network interface on the Gray Network Firewall:

      i) Select a device on the network connected to that interface of the Gray Network Firewall. Hereafter the device will be called Device A.

      ii) Select a device on the network connected to an interface of the Gray Network Firewall that Device A is not connected to. Hereafter the device will be called Device B.

      iii) Select a device on the network connected to an interface of the Gray Network Firewall that Device A is not connected to, and that Device B is allowed to communicate with. Hereafter the device will be called Device C.

      iv) Place a network sniffer between the Gray Network Firewall and Device C.

      v) Configure Device A to use the IP address of Device B.

      vi) Attempt to send traffic from Device A (spoofing Device B's IP address) to Device C, of a type that Device B is allowed to send to Device C.

      vii) Verify that the packet sniffer did not observe any packets with a source address of Device B and a destination address of Device C. (VPN-FW-8)

      viii) Verify that the Gray Network Firewall logs contain an event for a packet received on the physical interface through which Device A connects, with a source address of Device B and a destination address of Device C. (VPN-AU-29)

Expected Results:

Each Gray Network Firewall detects the use of spoofed addresses and does not allow packets with spoofed source addresses from passing through, even if non-spoofed traffic from that source address would be allowed.

14.19 Gray Network Firewall HTTP Deep Packet Inspection

This section contains a procedure for ensuring that the deep packet inspection performed by the Gray Network Firewalls is configured so only the specific types of HTTP traffic desired between Inner VPN Components and Inner CDPs is allowed.

Requirements being tested: VPN-AU-29, VPN-FW-3, VPN-FW-4, VPN-FW-9

Procedure Description:

1) For each Inner VPN Component within the solution:

a) For each Inner CDP within the solution:

i) Attempt to have the Inner VPN Component download the current CRL from the Inner CDP.

ii) Verify that the download was successful. (VPN-FW-3, VPN-FW-4)

iii) Identify the first Gray Network Firewall on the physical path from the Inner VPN Component to the Inner CDP. If no such Gray Network Firewall exists, skip the remainder of Step 1(a).

iv) Replace the CRL on the Inner CDP with a text file.

v) Place a packet sniffer on the interface of the Gray Network Firewall facing the Inner VPN Component.

vi) Attempt to have the Inner VPN Component download the current CRL from the Inner CDP.

vii) Verify that the request failed.

viii) Verify that the packet sniffer did not record any packets with a source address of the Inner CDP and a destination address of the Inner VPN Component that contains an HTTP response payload. (VPN-FW-4)

ix) Verify that the Gray Network Firewall logs contain an event for an improper HTTP response payload with a source address of the Inner CDP and a destination address of the Inner VPN Component. (VPN-AU-29)

x) Restore the CRL on the Inner CDP.

xi) Move the packet sniffer to the interface of the Gray Network Firewall facing the Inner CDP.

xii) Attempt to have the Inner VPN Component download a CRL from the Inner CDP using an incorrect URL.

xiii) Verify that the request failed.

xiv) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Component and a destination address of the Inner CDP. (VPN-FW-3)

xv) Verify that the Gray Network Firewall logs contain an event for an improper HTTP request with a source address of the Inner VPN Component and a destination address of the Inner CDP. (VPN-AU-29)

xvi) Attempt to have the Inner VPN Component issue an HTTP POST request for the URL of the CRL on the Inner CDP.

xvii) Verify that the request failed.

xviii) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Component and a destination address of the Inner CDP. (VPN-FW-3)

xix) Verify that the Gray Network Firewall logs contain an event for an improper HTTP request with a source address of the Inner VPN Component and a destination address of the Inner CDP. (VPN-AU-29)

b) For every other device on the Gray network that is not an Inner CDP, follow the procedure for Step 1(b) in Section 14.16. (VPN-AU-29, VPN-FW-9)

Expected Results:

In Step 1(a), the Gray Network Firewall allows only HTTP traffic between the Inner VPN Component and Inner CDP that consists of a GET request for the appropriate CRL and a response containing the CRL. In Step 1(b), the Gray Network Firewall denies HTTP requests from the Inner VPN Component to devices that are not Inner CDPs.

14.20 CRL Configuration for CDPs

This section contains procedures to ensure that the CRL configurations for the CDPs used within the VPN solution follow the requirements given in this Capability Package.

Requirements being tested: VPN-CD-1 through VPN-CD-15 and VPN-AU-26 through VPN-AU-28

Procedure Description:

1) Verify that the CRL hosted by the Outer CDP does not contain extensions other than those specified in RFC5280. (VPN-CD-01)

   a) Pull down a valid CRL from the Gray Network CA.

   b) Verify that the CRL does not contain any fields that are not specified in RFC5280.

2) Verify that the CRL hosted on the Inner CDP is signed by the Red Network CA. (VPN-CD-2) (VPN-CD-12)

   a) Download the CRL from the Inner CDP.

   b) Verify that the CRL is signed by the Red Network CA.

3) Verify that the CRL hosted on the Outer CDP is signed by the Gray Network CA. (VPN-CD-3) (VPN-CD-13)

   a) Download the CRL from the Outer CDP.

b) Verify that the CRL is signed by the Gray Network CA.

4) Verify that the Inner and Outer CDPs are only issuing CRLs over port 80. (VPN-CD-4)

   a) Perform a port scan on the Inner and Outer CDP and verify that the only open ports are 80 and the port used for management of the devices.

5) Verify that the implementing organization's policy describes an approved one way mechanism for transferring CRLs from the Red Network CA to the Inner CDP Server. (VPN-CD-5)

6) Verify that the implementing organization's policy describes an approved one way mechanism for transferring CRLs from the Gray Network CA to the Outer CDP Server. (VPN-CD-6)

7) Verify that the implementing organization has an approved policy in place that states a new CRL shall be transferred to a CDP server at least 4 days prior to the expiration of the current CRL and who will perform this action. (VPN-CD-7)

8) Verify that the VPN Gateway has checked the age of the current cached CRL prior to an establishment of a new connection. (VPN-CD-8)

   a) Log into the VPN Gateway and verify that it is configured to check the age of the current cached CRL prior to establishment of a new connection.

   b) Load a CRL with an age of greater than 1 hour onto a VPN Gateway.

   c) Establish a new connection between sites.

   d) Inspect CRL on the VPN Gateway.

9) Verify that the VPN Gateways are able to load the CDP CRL at least 3 days prior to the expiration of the current CRL. (VPN-CD-9)

   a) Log into the VPN Gateway and verify that it is configured to load the CDP CRL at least 3 days prior to the expiration of the current CRL.

   b) Load a CRL that is set to expire within 3 days.

   c) Establish a new connection between sites.

   d) Inspect CRL on the VPN Gateway.

10) Verify that the CDP only allows outbound traffic on port 80 and ports used for remote management traffic that adheres to VPN-RA-1. (VPN-CD-10)

a) Log into the CDP and verify that it is configured to only allow outbound traffic on port 80 and ports used for remote management traffic in accordance with VPN-RA-1.

11) Verify that traffic filtering rules on the Inner and Outer CDPs are applied based on known VPN Gateway addresses. (VPN-CD-11)

a) Remove a valid VPN Gateway from the whitelist.

b) Have the removed VPN Gateway attempt to download the CRL from the CDP.

c) Verify that the download fails.

12) Verify that the current CRL cached is used if integrity check of the CRL pulled from the CDP fails. (VPN-CD-14)

a) Working with two Inner VPN Gateways (Gateway A and B) with valid certificates, load a valid CRL that will soon expire onto both Gateway A and B.

b) Revoke the certificate for Gateway B.

c) Issue a new CRL.

d) Modify the CRL file.

e) Load the modified CRL file on the CDP.

f) Have Gateway A connect to Gateway B.

g) Verify that the connection was successful.

h) Review the Gateway audit logs to verify that the modified CRL was downloaded and a validity check occurred and failed.

13) Verify that the implementing organization has an approved policy in place that states that the VPN Gateway is manually updated prior to the expiration of the current CRL if the CDP is down or contains a bad CRL. (VPN-CD-15)

14) Verify that the VPN Components log the failure to pull the CRL from the Inner or Outer CDP. (VPN-AU-26)

a) CDP Servers shall remove all CRLs.

b) VPN Components shall attempt to pull the CRL from their respective CDPs.

c) Review the VPN Components audit logs to verify that a log report is generated from failure to pull the CRL.

15) Verify that the VPN Components log if the version of the CRL on the Inner or Outer CDP is older than the current cached CRL. (VPN-AU-27)

    a) Load the CDPs with CRLs that are older than the current cached CRLs on the VPN Components.

    b) Have the VPN Components attempt to pull the CRLs.

    c) Review the VPN Component audit logs to verify that a log report is generated.

16) Verify that the VPN Components log if signature validation of the CRL on the Inner or Outer CDP fails. (VPN-AU-28)

    a) Load the CDPs with CRLs that contain an invalid signature.

    b) Have the VPN Components pull the CRLs.

    c) Review the VPN Component audit logs to verify that a log report is generated due to an invalid CRL signature.

Expected Results:

For step 1, the CRL should only contain fields specified in RFC5280. For steps 2-3, the CRL hosted on the Inner and Outer CDP shall be signed by the Red Network CA and Gray Network CA respectively. For step 4, the Inner and Outer CDP CRL's should only be issued on port 80. For steps 5-7 & 13, the implementing organization should have policies in place to address the requirements identified. For steps 8-9, the VPN Gateway should retrieve a new CDP CRL. For step 10, the CDP will only allow outbound traffic on port 80 and ports used for remote management traffic. For step 11, the VPN Gateway's attempt to download a CRL should fail. For step 12, the current CRL cached should be used. For steps 14-16, there should be an audit log entry created for each requirement.

APPENDIX A. GLOSSARY OF TERMS

Accreditation – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

Assurance – A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. Certification by designated technical personnel of the extent to which design and implementation of the system meet specified technical requirement for achieving adequate data security.

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit Log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective action are required.

Availability – Assurance that the system and its associated assets are accessible and protected against denial or service attacks, as well as available when the user needs them and in the form needed by the user.

Black Box Testing – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

Black Network – A network that contains classified data that has been encrypted twice. (See Section 4.1.3)

Capability Package – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. This package will point to potential products that can be used as part of this solution.

Central Management Site – A site within a VPN solution that is responsible for remotely managing the solution components located at other sites. (See Section 4.3.1.2)

Certification – The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Certification and Accreditation (C&A) – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37).

Certificate Authority (CA) – An authority trusted by one or more users to create and assign certificates. [ISO9594-8]

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [RFC 3647]

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Confidentiality – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure and confidence in that only the appropriate set of individuals or organizations would be provided the information.

Control Plane Protocol – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

CRL Distribution Point (CDP) – A web server that hosts a copy of a CRL issued by a CA for VPN Components to download. (See Section 5.7)

Cross Domain Solution (CDS) – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. [CNSSI 4009]

Designated Approving Authority (DAA) – The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk, synonymous with designating accrediting authority and delegated accrediting authority. [CNSSI 4009]

End User Device (EUD) – The component which users directly interact with and which terminates one or both IPsec VPN tunnels. (See Section 5.5)

External Interface – The interface on a VPN Gateway that connects to the outer network (i.e., the Gray network on the Inner VPN Gateway or the Black network on the Outer VPN Gateway).

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Box Testing – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e., knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

Gray Network – A network that contains classified data that has been encrypted once. (See Section 4.1.2)

Gray Network Firewall – A stateful traffic filtering firewall placed on the Gray network to provide additional separation between flows of singly-encrypted data of different classification levels. (See Section 5.6)

Independently Managed Site – A site within a VPN solution whose solution components are locally managed and that does not remotely manage other sites' solution components. (See Section 4.3.1.1)

Internal Interface – The interface on a VPN Gateway that connects to the inner network (i.e., the Gray network on the Outer VPN Gateway or the Red network on the Inner VPN Gateway).

Local End User Device (EUD) – An EUD that is used exclusively within secure physical environments. (See Section 5.5.1)

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Red Network – A network that contains unencrypted classified data. (See Section 4.1.1)

Remote End User Device (EUD) – An EUD that is used outside of a secure physical environment. (See Section 5.5.2)

Remote Site – A site within a VPN solution whose solution components are remotely managed by a Central Management Site. (See Section 4.3.1.2)

Security Level – The combination of classification level, list of compartments, dissemination controls, and other controls applied to the information within a network.

VPN Client – A VPN application installed on an EUD.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – The VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in secure facility and includes Inner and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include EUDs.

APPENDIX B. ACRONYMS

Acronym	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
AO	Authorizing Official
ARP	Address Resolution Protocol
BFD	Bidirectional Forwarding Detection
C&A	Certification and Accreditation
CA	Certificate Authority
CAA	Certificate Authority Administrator
CCI	Controlled Cryptographic Item
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority
DAR	Data-at-Rest
DDoS	Distributed Denial of Service
DH	Diffie Hellman
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
EUD	End User Device
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards
GOTS	Government Off-the-Shelf
GRE	Generic Routing Encapsulation
HAIPE	High Assurance Internet Protocol Encryption
HTTP	Hypertext Transfer Protocol

Acronym	Definition
HTTPS	Hypertext Transfer Protocol Secure
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alerts
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
MLD	Multicast Listener Discovery
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
OID	Object Identifier
OS	Operating System
OSPF	Open Shortest Path First
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
RFC	Request for Comment
RSA	Rivest Shamir Adelman algorithm
S3	Secure Sharing Suite
SA	Security Association
SCRM	Supply Chain Risk Management
SHA	Secure Hash Algorithm
SIPRNet	Secret Internet Protocol Router Network
SP	Service Packs
SSH	Secure Shell
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VM	Virtual Machine
VPN	Virtual Private Network

APPENDIX C. REFERENCES

CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems* www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2010
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	March 2010
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000)*	June 2009
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
IPsec VPN Client PP	*IPsec VPN Client Protection Profile*. www.niap.ccevs.org/pp	January 2012
NSA Suite B	*NSA Guidance on Suite B Cryptography [including the Secure Sharing Suite (S3)]*. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force http://www.ietf.org/rfc/rfc3647.txt	November 2003
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006

RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman	December 2005
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley.	January 2012
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
SP 800-56A	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, D. Johnson, and M. Smid	March 2007
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	January 2011

SP 800-147 *NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et. al. April 2011

APPENDIX D. EXAMPLE IAD APPROVAL LETTER FOR VPN CAPABILITY PACKAGE SOLUTIONS

A sample IAD approval letter will be provided in a future version of this Capability Package.

APPENDIX E. END USER DEVICE IMPLEMENTATION NOTES

End User Devices (EUDs) that physically connect to the Black network contain an Inner VPN Client and an Outer VPN Clients, both of which are needed to provide the user with remote access to a classified network. Although this Capability Package levies several requirements on the EUD, it does not specify how to design the EUD itself in order to meet those requirements. System developers have flexibility in choosing how to design their EUDs, as long as they comply with this Capability Package's requirements.

EXAMPLE EUD IMPLEMENTATION APPROACHES

This appendix lists example design choices that system developers can make when implementing EUDs that will physically connect to a Black network, and is intended for illustrative purposes only. Following one of the designs in this appendix is **not** a requirement for compliance with this Capability Package, and although acceptable, does **not** by itself guarantee that the resulting implementation necessarily complies with all of the requirements of this Capability Package.

For an EUD that physically connects directly to the Black network, there is no physical Gray or Red network on its side of the VPN connection. However, data flows within the EUD can be considered Red, Gray, or Black based on the number of layers of encryption that have been applied to the data.

EXAMPLE 1: VIRTUALIZATION USING TYPE 2 (HOSTED) HYPERVISOR

The first example for implementing the EUD is to use virtualization to run the Inner and Outer VPN Clients on separate operating systems (OSes). Since each OS implements its own IP stack, the design meets requirement VPN-EU-5. Running the Inner and Outer VPN Clients on separate OSes also prevents them from using the same private key store, meeting requirement VPN-EU-4.

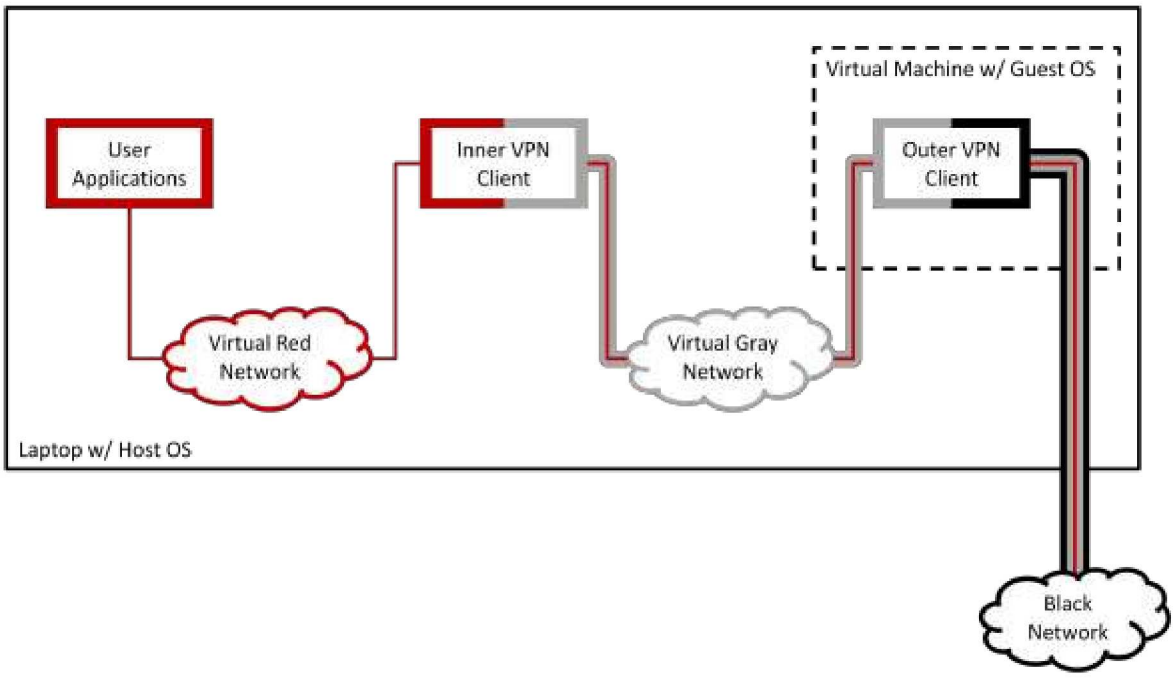


Figure 12. Example EUD Implementation Using a Type 2 Hypervisor

In this example, illustrated in Figure 12, the EUD is an ordinary laptop running a virtual machine (VM) on a Type 2 (hosted) hypervisor. The Outer VPN Client runs within the virtual machine on top of the guest OS. The Inner VPN Client and the user applications both run outside of the virtual machine, on top of the host OS.

The laptop's physical network interface is bridged directly to the virtual machine, preventing applications (other than the virtual machine itself) from directly communicating over the Black network. The virtual machine software creates a virtual network between the host and guest OSes which acts as the Gray network within the EUD; the host and guest OSes each have a virtual network interface to this network. The Inner VPN Client also creates an additional virtual network interface on the host OS, which the user applications will connect to; this virtual network acts as the Red network within the EUD.

The host OS is configured to only allow the Inner VPN Client to connect to the virtual Gray network interface. The host OS's routing table forces all other network traffic through the virtual Red network interface. The Inner VPN Client encrypts all data sent through this interface and forwards it to the virtual Gray network into the guest OS, where the Outer VPN Client encrypts it a second time before sending it out the bridged physical interface to the Black network. Traffic arriving at the EUD follows the reverse path to be decrypted twice before being provided to the user applications.

The guest OS can implement packet filtering on both its Gray and Black network interfaces. The packet filter on the Gray interface would block all traffic except IKE, ESP, and remote management protocols.

The packet filter on the Black interface would block all traffic except IKE, ESP, and protocols such as DHCP or DNS needed to join the Black network and connect to the Outer VPN Gateway.

EXAMPLE 2: VIRTUALIZATION USING TYPE 1 (NATIVE) HYPERVISOR

The second example for implementing the EUD also involves the use of virtualization to run the Inner and Outer VPN Clients on separate OSes. This example takes the approach further by using a Type 1 (native) hypervisor to run the Outer VPN Client, Inner VPN Client, and user applications each in their own virtual machines, as shown in Figure 13.

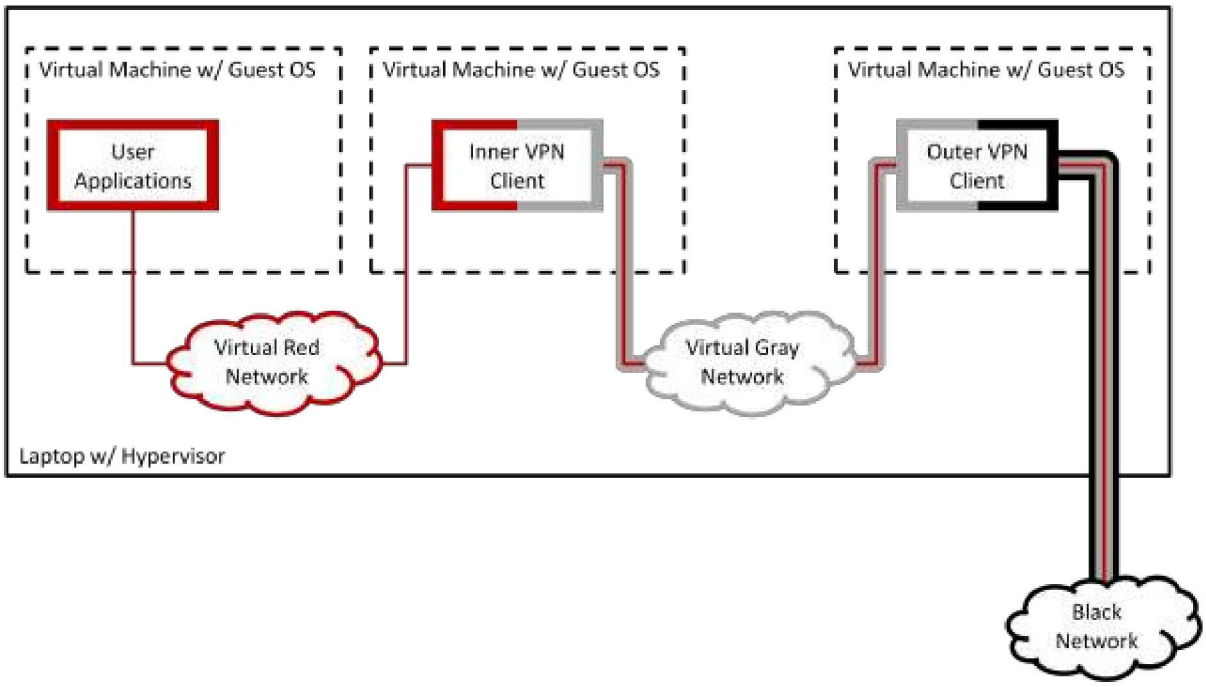


Figure 13. Example EUD Implementation Using a Type 1 Hypervisor

As in the first example, the laptop's physical network interface is bridged directly to the virtual machine that contains the Outer VPN Client. The hypervisor creates two virtual networks: a virtual Gray network between the VM for the Outer VPN Client and the VM for the Inner VPN Client, and a virtual Red network between the VM for the Inner VPN Client and the VM for the user applications. The virtual network configuration forces all traffic leaving the user applications to go through both the Inner and Outer VPN Clients before passing over the Black network.

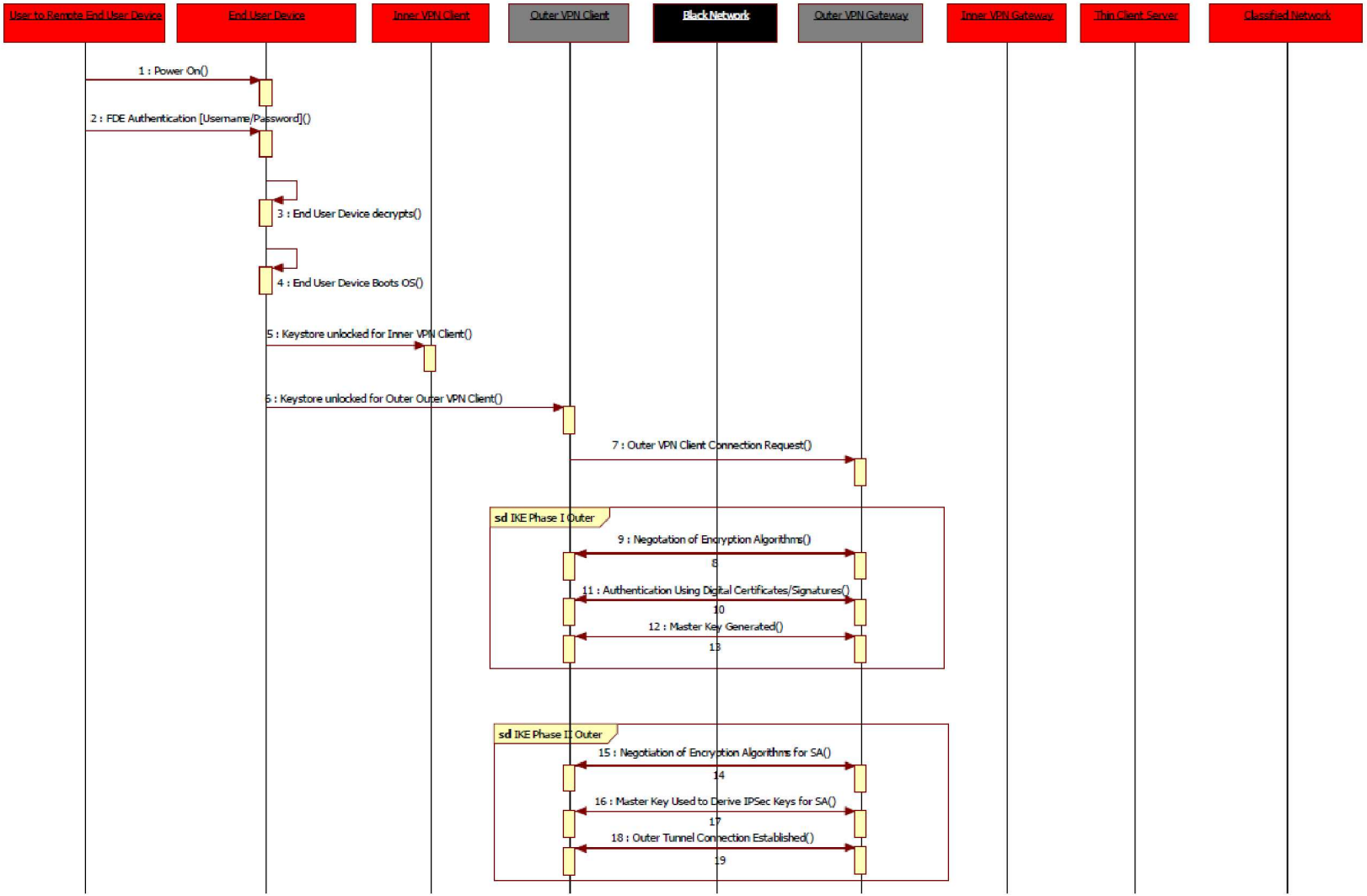
The guest OSes for the Inner and Outer VPN Clients could implement packet filtering for each of their interfaces, or the packet filtering could be performed by the hypervisor. Packet filters for the virtual Red network would block all traffic except for the protocols needed for approved user applications and for remote management. Packet filters for the virtual Gray network would block all traffic except for IKE, ESP, and remote management protocols. Packet filters for the Black network would block all traffic

except IKE, ESP, and protocols such as DHCP or DNS needed to join the Black network and connect to the Outer VPN Gateway.

UML Sequence Diagram for EUD Tunnel Establishment

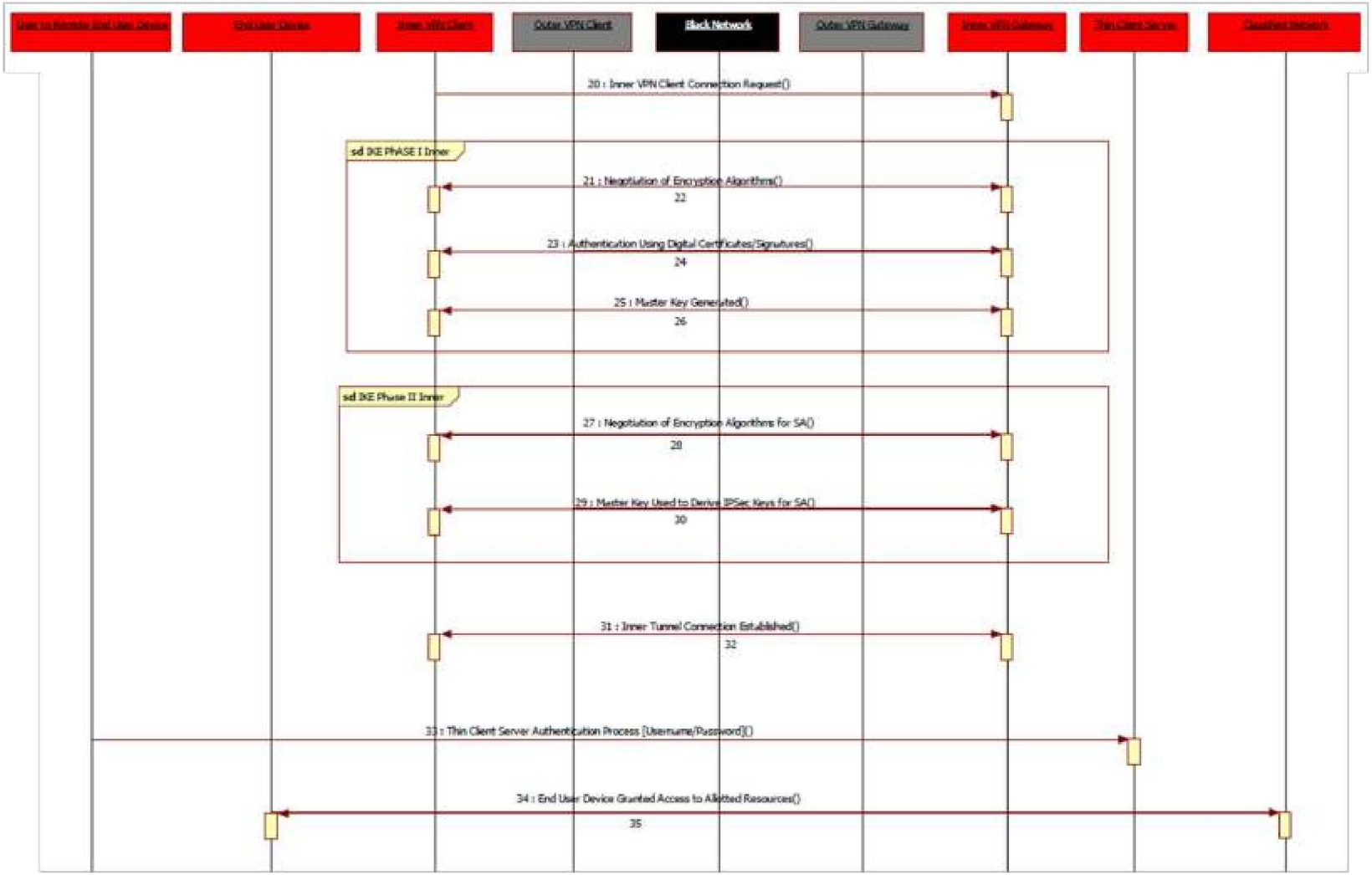
The Unified Modeling Language (UML) sequence diagram below illustrates one possible sequence of events an EUD might take from power-up to the user accessing classified data through the solution. The diagram shows how the parts of the EUD interact with components in the infrastructure site to establish the tunnels and authenticate the user.

Virtual Private Network Capability Package



Continued on next page

Virtual Private Network Capability Package



APPENDIX F. SUMMARY OF CHANGES TO REQUIREMENTS

This appendix summarizes the changes between the requirements in this Capability Package and the requirements in its predecessor, the CSfC VPN Capability Package version 2.0, dated May 28, 2013. It is provided as an aide to solution owners who have developed a solution compliant with the earlier Capability Package and wish to determine the extent to which their existing solution complies with this Capability Package.

In general, requirements included in the CSfC VPN Capability Package version 2.0, dated May 28, 2013, are also included in this Capability Package without any substantive changes. The wording used in several requirements has been changed to clarify their intent, and typically a solution that complied with their original wording is expected to also comply with their revised wording.

Most of the new requirements added in this Capability Package only apply to the two new optional capabilities introduced in this Capability Package, described in Sections 4.3.3.3 and 4.3.4. The primary exception to this is the addition of new requirements addressing the content and distribution of CRLs (see Section 10.10.1) and new port filtering requirements (see Section 10.6), which apply to all solutions adhering to this Capability Package.

Table 22 lists in more detail which requirements from the CSfC VPN Capability Package version 2.0, dated May 28, 2013, have changed in this Capability Package. Any requirements not listed here have not changed.

Table 22. Changes to VPN CP 2.0 Requirements

VPN CP 2.0 Requirement	Change Description
VPN-CR-2	Renamed VPN-PF-10. Requirement text is unchanged.
VPN-CR-9	Rewritten to clarify the intended meaning of the requirement.
VPN-CR-13	Renamed VPN-PF-11. Requirement now applies to all network interfaces of VPN Components. Extraneous detail removed.
VPN-CR-14	Rewritten to clarify the intended meaning of the requirement.
VPN-CR-21	Modified to clearly allow solution owners to choose shorter IKE SA lifetimes.
VPN-CR-22	Modified to clearly allow solution owners to choose shorter ESP SA lifetimes.
VPN-PF-2	Modified to clearly allow approved management protocols through interfaces connected to the Gray network.
VPN-RA-1	Modified to clarify the intended meaning of the requirement.
VPN-RA-3	Modified to clarify the intended meaning of the requirement.
VPN-RA-4	Modified to clarify the intended meaning of the requirement.
VPN-RA-5	Modified to clarify the intended meaning of the requirement.

VPN CP 2.0 Requirement	Change Description
VPN-AU-21	Modified to clearly allow a single VPN Component to establish multiple VPN connections simultaneously.
VPN-AU-22	Modified to clearly allow a single VPN Component to establish multiple VPN connections simultaneously.
VPN-AU-23	Modified to clearly allow a single VPN Component to establish multiple VPN connections simultaneously.
VPN-KM-12	Modified to allow rekeying of VPN Gateways to be done through out-of-band means if desired.
VPN-KM-13	Superseded by VPN-KM-26, which requires more frequent distribution of revocation information.
VPN-GD-1	Modified to clarify the intended meaning of the requirement.
VPN-GD-4	Corrected error in architecture assignment. Requirement only applies to architectures incorporating EUDs.
VPN-GD-33	Removed portion dealing with CRLs, which is now addressed in VPN-KM-25 and VPN-KM-26.
VPN-GD-34	Superseded by VPN-KM-26, which applies more broadly and includes a time constraint.

Table 23 lists the new requirements added in this Capability Package that are applicable to the solution architectures from the CSfC VPN Capability Package version 2.0, dated May 28, 2013. It does not list the new requirements that apply solely to the solution architectures introduced in this Capability Package.

Table 23. New Requirements Applicable to VPN CP 2.0 Solution Architectures

VPN CP 2.08 Requirement	Architectures
VPN-CR-25	M, R, L
VPN-PF-12	M, R, L
VPN-PF-13	M, R, L
VPN-PF-14	M, R, L
VPN-KM-25	M, R, L
VPN-KM-26	M, R, L
VPN-KM-27	M, R, L
VPN-KM-28	M, R, L